(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 649 261 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
23.01.2002 Bulletin 2002/04

(51) Int Cl.[7]: **H04N 7/24**, H04N 7/167

(21) Application number: **94307609.1**

(22) Date of filing: **17.10.1994**

(54) Image data processing and encrypting apparatus

Vorrichtung zur Verarbeitung und Verschlüsselung von Bilddaten

Appareil pour le traitement et le chiffrage de données d'images

(84) Designated Contracting States:
DE ES FR GB IT NL

(30) Priority: **18.10.1993 JP 25977093**

(43) *Date of publication of application:*
19.04.1995 Bulletin 1995/16

(73) Proprietor: **CANON KABUSHIKI KAISHA**
Tokyo (JP)

(72) Inventor: **Enari, Masahiko,**
c/o Canon Kabushiki Kaisha
Ohta-ku, Tokyo (JP)

(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co. 2-5 Warwick Court, High Holborn
London WC1R 5DH (GB)

(56) References cited:
EP-A- 0 364 285
EP-A- 0 485 230
EP-A- 0 542 261
EP-A- 0 582 122
EP-A- 0 614 308
EP-A- 0 619 677
WO-A-94/15437

EP 0 649 261 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to an image processing apparatus, and more particularly to the encryption of image data.

[0002] Fig. 1 shows a block diagram of a configuration of a prior art image encoding apparatus having an encryption function.

[0003] Fig. 2 shows a block diagram of an image decoding apparatus for decoding the image data encoded by the apparatus of Fig. 1.

[0004] In the encoding apparatus shown in Fig. 1, numeral 110 denotes a high resolution analog video signal (hereinafter referred to as an HD signal), which, in the present example, has the number of scan lines of 1,050 and a frame frequency of 30 Hz. Relative to the HD signal, a video signal of an ordinary resolution having the number of scan lines of 525, a frame frequency of 30 Hz and the number of pixels of 858 is referred to as an SD signal.

[0005] An HD A/D conversion circuit 112 samples the video signal 110 at a sampling frequency of 54.054 MHz to convert it to a digital signal. By virtue of the sampling frequency, the number of pixels per line of the digital HD signal is 1,716. A high resolution (HD)/ordinary resolution (SD) conversion circuit 114 reduces the number of pixels to one half in both vertical direction and horizontal direction to output a video signal of the ordinary resolution having the number of scan lines of 525, the frame frequency of 30 Hz and the number of pixels per line of 858.

[0006] An encoding circuit 116 efficiently encodes the digital SD signal outputted from the conversion circuit 114 by an encoding scheme which is a combination of motion compensated adaptive prediction and DCT. A decoding circuit 118 decodes the encoded signal outputted from the decoded circuit 116 to reproduce an SD signal. An SD/HD conversion signal 120 interpolates pixels to the output video data from the decoding circuit 118 by a factor of two in both vertical direction and horizontal direction to convert it to an HD signal. Namely, the SD/HD conversion circuit 120 outputs a signal corresponding to the high resolution video signal having the number of scan lines of 1,050, the number of pixels per line of 1,716 and the frame frequency of 30 Hz.

[0007] A subtractor 122 subtracts the output of the SD/HD conversion circuit 120 from the output of the A/D conversion circuit 112 for each pixel. The output of the subtractor 122 is referred to as an auxiliary video signal. An encoding circuit 124 encodes the output of the subtractor 122 in the same encoding scheme as that for the encoding circuit 116.

[0008] A multiplexing circuit 126 multiplexes the encoded data (the encoded SD signal) outputted from the encoding circuit 116 and the encoded data (the encoded auxiliary video signal) outputted from the encoding circuit 124 and outputs it to an encryption circuit 128. The encryption circuit 128 encrypts the output of the multiplexing circuit 126 in accordance with an encryption key signal of an encryption key output circuit 130, and an output unit 132 outputs the encrypted data outputted from the encryption circuit 128 to a transmission line. As described above, the transmission line may be a communication line or a recording medium.

[0009] The encryption is briefly explained with reference to Figs. 3 and 4. Following encryption techniques are available.

[0010] Fig. 3 shows a flow chart of the encryption by the US Data Encryption Standard (DES) published in the FIPS Publication 46 dated January 15, 1977, and Fig. 4 shows a function of the encryption of Fig. 3. The data encryption algorithm of the DES has been published as the "Data Encryption Standard" as described above. Referring to Figs. 3 and 4, the DES will be explained.

[0011] The DES handles block encryption to binary data comprising 0's and 1's. In the DES, the binary data is grouped into 64-bit blocks and the transposition and the replacement are repeated for each block to encrypt it. An encryption key is a 64-bit signal, of which 8 bits are check bits for detecting an error. Thus, a 56-bit encryption key is actually effective. The replacement of the digit is controlled by the encryption key in each cycle. Fig. 3 shows an encryption process of the DES. Fig. 4 shows a function fK(R) which is a heart of the encryption.

[0012] As shown in Fig. 3, a 64-bit plain text is first transpositioned. This is a fixed transposition independent from the encryption key. Then, the 64 bits are divided into a left half L_0 and a right half R_0. Then, the following operations are repeated over the 16 stages:

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} + fK_n(R_{n-1}) \quad (1)$$

where + represents a sum of mode 2 for each bit, L_n and R_n represent the left half 32 bits and the right half 32 bit, respectively, at the end of the operation for the n-th stage, and K_n is generated from the encryption key as shown in the right side of Fig. 3. In Fig.3 $s_1 \ldots s_{16}$ are 1 or 2.

[0013] Condensed transposition is defined as the transposition excluding some of the input. In Fig. 3, 8 bits out of the 56 input bits are excluded so that an output comprises 48 bits. The condensed transposition is irrevocable conversion so that the input cannot be perfectly reproduced from the output. This serves to make the estimation of the encryption key difficult.

[0014] Referring to Fig. 4, the function fK(R) in Fig. 3 is specifically explained. In Fig. 4, to generate the function fK(R), augmented transposition is made to R. The augmented transposition is defined as the overlapped transposition of some inputs. In the illustrated example, 16 bits out of the 32 input bits appear in overlap at the

output. K composed by the key is mode 2 added to the output. The resulting 48 bits are divided into eight 6-bit blocks and the respective 6 bits are converted to 4 bits by S_1, S_2, ..., S_8, respectively. Assuming that the 6 bits constitute one character, it may be considered as a kind of replacement. However, since the output is compressed to 4 bits, the conversion is irrevocable. Accordingly, the fK(R) is generally an irrevocable function. This, however, does not mean that the conversion of the formula (1) is irrevocable. The formula (1) may be converted as follows:

$$R_{n-1} = L_n$$

$$L_{n-1} = R_n + fK_n(R_{n-1})$$

$$= R_n + fK(L_n) \qquad (2)$$

It is thus seen that L_{n-1} and R_{n-1} can be calculated from L_n and R_n.

[0015] The calculation of the formula (1) is repeated 16 times and when L_{16} and R_{16} are determined, they are finally transpositioned again and the encryption is terminated.

[0016] In a decoding apparatus shown in Fig. 2, a transmission data input unit 140 receives the data from the transmission line and supplies it to a decryption circuit 142. The decryption circuit 142 decrypts it by utilizing the encryption key signal outputted from the encryption key output circuit 144. In order for the decryption to be correctly done, the exactly same encryption key as that outputted from the encryption key output circuit 130 used in the encoding apparatus (see Fig. 1) should be used.

[0017] The decryption is substantially a reverse operation to the encryption. Briefly, the process proceeds from the bottom to the top in Fig. 3. First, a reverse transposition to the last transposition in the encryption is made, and R_{n-1} and L_{n-1} are determined from the formula (2), and when R_0 and L_0 are determined, a reverse transposition to the first transposition in the encryption is made. In this manner, the original 64 bits are reproduced. In order to decrypt the DES encrypted text, there has been no known method other than examining the keys one by one. Assuming that one microsecond is needed to examine if one key is correct one or not, 2,283 years will be needed to examine all of 2^{56} keys.

[0018] The transmission data decrypted by the decryption circuit 142 is separated by a separation circuit 146 to encoded data of the SD signal and encoded data of the auxiliary video signal, which are supplied to decoding circuits 148 and 150, respectively. The decoding circuit 148 outputs the reproduced SD signal and the decoding circuit 150 output the reproduced auxiliary video signal.

[0019] An SD A/D conversion circuit 152 converts the digital SD signal outputted from the decoding circuit 148 to an analog signal. The output of the SD A/D conversion circuit 152 is an analog video signal having the number of scan lines of 525 and the frame frequency of 30 Hz. This video signal is applied to a monitor device of an ordinary resolution to display the image.

[0020] An SD/HD conversion circuit 154 converts the digital SD signal outputted from the decoding circuit 148 to a digital HD signal in the same process as that of the SD/HD conversion circuit 120. An adder 156 adds the output of the decoding circuit 150 and the output of the SD/HD conversion circuit 154. The output of the adder 156 is a video signal corresponding to the high resolution video signal. An HD D/A conversion circuit 158 converts the digital output of the adder 156 to an analog signal. The output of the HD D/A converter 158 is a video signal having the number of scan lines of 1,050 and the frame frequency of 30 Hz. The video signal is applied to a high resolution monitor to display the image.

[0021] The above prior art video signal encoding and decoding apparatus has a problem in that the video signal cannot be reproduced for those who do not have the encryption key, for both the low resolution video signal and the high resolution video signal.

[0022] There is a demand that charges to users are discriminated between the low resolution display device having the number of scan lines of 525 and the high resolution display device having the number of scan lines of 1,050, for the same content, but the prior art apparatus does not meet the requirement.

[0023] It is known from EP-A-0364285 to divide a television signal into a number of spatiotemporal components and to perform scrambling on those components containing high frequencies in order to reduce the effects of random noise and interference.

[0024] The following references WO-A-94/15437, EP-A-0582122, EP-A-0614308 and EP-A-0619677 are cited against the present application as prior art only to the extent provided by Articles 54(3) and (4) EPC. WO-A-94/15437 discloses partial unscrambling and decoding of a scrambled television signal by receivers having partial access rights.

[0025] EP-A-0582122 discloses scrambling apparatus for encoded video data.

[0026] EP-A-0614308 discloses key encryption of selected image components such that access to low resolution components is available without decryption.

[0027] EP-A-0619677 discloses scrambling of direct cosine transformation coded blocks of video data, including the scrambling of a DC component.

[0028] According to the present invention there is disclosed an image processing apparatus as set out in claim 1.

[0029] Acording to other aspects of the invention there is also disclosed apparatus and method as set out in claims 6, 13 and 18. Further aspects of the invention are set out in the dependend claims.

[0030] Other aspects features and advantages of the

invention will become apparent from the following detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031]

Fig. 1 shows a block diagram of a prior art image encoding apparatus,
Fig. 2 shows a block diagram of a prior art image decoding apparatus,
Fig. 3 shows a flow of prior art encryption,
Fig. 4 shows a flow of prior art encryption,
Fig. 5 shows a block diagram of a configuration of one embodiment of an image encoding apparatus of the present invention,
Fig. 6 shows a block diagram of a configuration of an embodiment of an image decoding apparatus of the present invention,
Fig. 7 shows a block diagram of a modified portion of a configuration of a modified embodiment of Fig. 6,
Fig. 8 shows a block diagram of a modified portion of a modified embodiment of Fig..6,
Fig. 9 shows a block diagram of a configuration of a second embodiment of the image encoding apparatus of the present invention,
Fig. 10 shows a block diagram of a configuration of a second embodiment of the image decoding apparatus of the present invention,
Fig. 11 illustrates band division of a space frequency,
Fig. 12 shows a block diagram of a configuration of a modified portion of a modified embodiment of Fig. 10,
Fig. 13 shows a block diagram of a configuration of a modified portion of a modified embodiment of Fig. 10,
Fig. 14 shows a block diagram of a specific encoding circuit of the embodiment, and
Fig. 15 shows a block diagram of a specific decoding circuit of the embodiment.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0032] Fig. 5 shows a block diagram of a configuration of one embodiment of the encoding apparatus of the present invention, and Fig. 6 shows a block diagram of a configuration of the decoding apparatus.

[0033] The encoding apparatus shown in Fig. 5 is first explained. Numeral 10 denotes a high resolution video signal having the number of scan lines of 1,050 and the frame frequency of 30 Hz as the HD signal 110 does. Numeral 12 denotes an HD A/D conversion circuit for converting the video signal 10 to a digital signal, numeral 14 denotes a high resolution (HD)/ordinary resolution (SD) conversion circuit for converting the digital HD signal outputted from the HD A/D conversion circuit 12 to a video signal of the ordinary resolution, numeral 16 denotes an encoding circuit for efficiently encoding the output of the conversion circuit 14, numeral 18 denotes a decoding circuit for decoding the output of the encoding circuit 16, numeral 20 denotes an SD/HD conversion circuit for interpolating the SD signal output of the decoding circuit 18 to convert it to an HD signal, numeral 22 denotes a subtractor for subtracting the output of the SD/HD conversion circuit 20 from the output of the HD A/D conversion circuit 12 for each pixel, and numeral 24 denotes an encoding circuit for encoding the output of the subtactor 22. The circuits 12 - 24 have the same functions as those of the circuits 112 - 124 of Fig. 1 and operate in the same manner.

[0034] Numeral 26 denotes an encryption circuit for encrypting the output of the encoding circuit 24 in accordance with an encryption signal outputted from an encryption key output circuit 28. As the encryption technique, the one which complies with the DES standard is used.

[0035] Numeral 30 denotes a multiplexing circuit for multiplexing the output of the encoding circuit 16 and the encryption circuit 26, and numeral 32 denotes an output unit for outputting transmission data multiplexed by the multiplexing circuit 30 to a transmission line such as a communication line or a recording medium.

[0036] The encoding apparatus shown in Fig. 5 is explained. The operations of the circuits 12 - 24 are same as those of the prior art apparatus. Namely, the encoding circuit 16 outputs the encoded data of the video signal derived by converting the HD signal 10 to the ordinary resolution, and the encoding circuit 24 outputs the encoded data of the auxiliary video signal to reproduce the high resolution video signal from the transmission video data of the ordinary resolution. In the present embodiment, prior to the multiplexing of the both encoded data, the output encoded data of the encoding circuit 24 is encrypted by the encryption circuit 26 by using the encryption key signal outputted from the encryption key output circuit 28 and it is applied to the multiplexing circuit 30.

[0037] Accordingly, in the present embodiment, the multiplexing circuit 30 multiplexes the encoded data of the video signal of the ordinary resolution (the output of the encoding circuit 16) and the encoded data of the encrypted auxiliary video signal and the output unit 32 outputs the output of the multiplexing circuit 30 to the transmission line. Accordingly, the video signal of the ordinary resolution is transmitted without encryption but the information for reproducing the high resolution video signal (auxiliary video signal) is encrypted so that, in the receiving station, the high resolution video signal cannot be reproduced without the encryption key but the video signal of the ordinary resolution can be reproduced without the encryption key.

[0038] The decoding apparatus shown in Fig. 6 is explained. Numeral 40 denotes a transmission data input

unit for receiving data from the transmission line, numeral 42 denotes a separation circuit for separating a set stream from the transmission data input unit 40 to a portion related to the encoded data of the SD signal and a portion related to the encoded data of the auxiliary video signal, and numeral 44 denotes a decryption circuit for decrypting the encoded data of the auxiliary video signal from the separation circuit 42 by referencing the encryption key signal outputted from the encryption key output circuit 46.

[0039] Numeral 48 denotes a decoding circuit for decoding the encoded data of the SD signal from the separation circuit 42, numeral 50 denotes a decoding circuit for decoding the encoded data of the auxiliary video signal from the decryption circuit 44, numeral 52 denotes an SD D/A conversion circuit for converting the digital SD signal outputted from the decoding circuit 48 to an analog signal, numeral 54 denotes an SD/HD conversion circuit for converting the digital SD signal outputted from the decoding circuit 48 to a digital HD signal in the same process as that of the SD/HD conversion circuit 20, numeral 56 denotes an adder for adding the output of the decoding circuit 50 to the output of the SD/HD conversion circuit 54, and numeral 58 denotes an HD D/A conversion circuit for converting the digital output of the adder 56 to an analog signal.

[0040] An operation of the decoding circuit shown in Fig. 6 is explained. The transmission data input unit 40 receives the data from the transmission line and supplies it to the separation circuit 42, and the separation circuit 42 separates it to a portion related to the encoded data of the SD signal and a portion related to the encoded data of the encrypted auxiliary video signal and supplies the former to the decoding circuit 48 and the latter to the decryption circuit 44. The decryption circuit 44 decrypts the encryption applied to the encoded data of the auxiliary video signal by using the same encryption key signal outputted from the encryption key output circuit 46 as the encryption key signal outputted from the encryption key output circuit 28 of the encoding circuit (Fig. 1). The encoded data of the auxiliary video signal decrypted by the decryption circuit 44 is applied to the decoding circuit 50 and decoded thereby.

[0041] Thus, the decoding circuit 48 outputs the reproduced digital SD signal and the decoding circuit 50 outputs the reproduced digital auxiliary video signal.

[0042] The SD D/A conversion circuit 52 converts the digital SD signal outputted from the decoding circuit 48 to an analog signal. The SD D/A conversion circuit 52 may be an analog signal having the number of scan lines of 525 and the frame frequency of 30 Hz and the video signal is applied to a monitor device of the ordinary resolution to display the image.

[0043] The SD/HD conversion circuit 54 converts the digital SD signal outputted from the decoding circuit 48 to a digital signal in the same process as that of the SD/HD conversion circuit 120. The adder 56 adds the output of the decoding circuit 50 to the output of the SD/HD conversion circuit 54 for each pixel. The output of the adder 56 is a video signal corresponding to the high resolution video signal. The HD D/A conversion circuit 58 converts the digital output of the adder 56 to an analog signal. The output of the HD D/A conversion circuit 58 is a high resolution video signal having the number of scan lines of 1,050 and the frame frequency of 30 Hz and it may be applied to a high resolution monitor to display the image.

[0044] In the decoding apparatus shown in Fig. 6, without the encryption key or if the encryption key is not correct (hereinafter collectively referred to as without key or no key state), the decryption circuit 44 outputs quite an unstable data pattern so that the output of the HD D/A conversion circuit 58 is also unstable and an unstable pattern such as a noise image is displayed on the screen of the display device such as a CRT.

[0045] Alternatively, a fixed image may be displayed on the high resolution monitor screen in the no key state. Figs. 7 and 8 show portions of block diagrams of such modified encoding apparatus. The like elements in Figs. 7 and 8 are designated by like numerals.

[0046] In Fig. 7, a switch 60 is provided between the decoding circuit 50 and the adder 56, and when the no key state (no input of the encryption key signal) is detected by the decryption circuit 44, the switch 60 is set to '0' by the detection output so that '0' is applied to the adder 56. When the correct encryption key is inputted to the decryption circuit 44', the decryption circuit 44' connects the switch 60 to the output of the decoding circuit 50.

[0047] In Fig. 8, a switch 62 is provided between the adder 56 and the HD D/A conversion circuit 58 so that in the no key state a predetermined level is inputted to the HD D/A conversion circuit 58. The switch 62 normally selects the output of the adder 56, and when the decryption circuit 44' the no key state (no input of the encryption key signal), the switch is set to the predetermined level input. In this manner, when the correct input is present, the high resolution video signal is outputted but in the no key state, the predetermined level signal is outputted and an image corresponding to the predetermined level is displayed on the monitor screen.

[0048] In Figs. 7 and 8, the switches 60 and 62 are illustrated to facilitate the understanding although it is apparent that the function of such switches 60 and 62 may be incorporated in the decoding circuit 50 and/or HD A/D conversion circuit 58. Alternatively, the output of the decoding circuit 50 or the HD D/A conversion circuit may be forced to a predetermined level (for example, zero output) in response to the detection of the no key state by the decryption circuit 44.

[0049] In Figs. 7 and 8, the no key state is detected by the decryption circuit 44 although it may be detected by error code detection or error correction process.

[0050] A second embodiment of the present invention which is applied to a system in which the image information is transmitted by the band division by the space

frequency is now explained. Fig. 9 shows a block diagram of a configuration of an encoding apparatus thereof, and Fig. 10 shows a block diagram of a configuration of a decoding apparatus. Fig. 11 illustrates the band division of the space frequency.

[0051] Numeral 210 denotes an analog HD signal to be encoded. In the present embodiment, it is a video signal having the number of scan lines of 1,050 and the frame frequency of 30 Hz. An HD A/D conversion circuit 212 samples the analog HD signal at a sampling frequency of 54.054 MHz to convert it to a digital signal. The number of pixels per line of the sampled HD signal is 1,716.

[0052] The output of the HD A/D conversion circuit 212 is applied to band division filters 214 and 216 and divided by the filters 214 and 216 to a low frequency component and a high frequency component at a horizontal frequency and the number of pixels is reduced to one half, respectively.

[0053] The output of the band division filter 214 is a low resolution component of the horizontal frequency, which is further separated into a low frequency component and a high frequency component at a vertical frequency by band division filters 218 and 220 to reduce the number of pixels to one half. Similarly, the band division filters 222 and 224 separates the output of the band division filter 216 (the high resolution component at the horizontal frequency) into a low frequency component and a high frequency component at the vertical frequency to reduce the number of pixels to one half.

[0054] In this manner, the high resolution video signal having 1,716 pixels in the horizontal direction and 1,024 pixels in the vertical direction is separated into an LL signal (the output of the band division filter 218), an LH signal (the output of the band division filter 220), an HL signal (the output of the band division filter 222) and an HH signal (the output of the band division filter 224) having one half of the total number of pixels in the horizontal direction and the vertical direction, as shown in Fig. 11. Since only the LL signal has the low-pass data in both the horizontal direction and the vertical direction, it is the video information which can be reproduced for display as the image and corresponds to the video signal of the ordinary resolution having the number of scan lines of 525, the frame frequency of 30 Hz and the number of pixels per line of 858. On the other hand, since the LH signal, the HL signal and the HH signal are high-pass data, they cannot be displayed as the image as they are and they are the auxiliary video signals which form the high resolution video signal in cooperation with the LL signal.

[0055] The encoding circuit 226 efficiently encodes the output of the band division filter 218 (LL signal) by an encoding scheme which is a combination of the motion compensated adaptive prediction known as the CCIR Recommendation 723 and the DCT. Encoding circuit 228, 230 and 232 efficiently encode the outputs of the band division filters 220, 222 and 224 (LH signal, HL signal and HH signal), respectively, by a combination of the DPCM and a zero run length encoded and variable length code. The outputs of the encoding circuits 228 - 232 are multiplexed by a multiplexing circuit 234. An encryption circuit 236 encrypts the output of the multiplexing circuit 234 by using the encryption key outputted from the encryption key output circuit 238 in accordance with the encryption technique of the DES standard described above.

[0056] The multiplexing circuit 240 multiplexes the output of the encoding circuit 226 and the output of the encryption circuit 236 and the output thereof is outputted to the transmission line by the output unit 242.

[0057] In the decoding apparatus shown in Fig. 10, the transmission data input unit 250 receives the transmission data from the transmission line and applies it to the separation circuit 252. The separation circuit 252 separates it into a portion related to the encoded data of the LL signal and a portion related to the other LH, HL and HH signals, and applies the former to the decoding circuit 254 and the latter to the decryption circuit 256. The decryption circuit 256 decrypts the encoded data of the LH, HL and HH signals by using the encryption key signal outputted from the encryption key output circuit 258. In order to correctly decrypt it, the encryption key should be same as that used for encoding the encryption key signal.

[0058] The separation circuit 260 separates the output of the decryption circuit 256 to the encoded data of the LH signal, the encoded data of the HL signal and the encoded data of the HH signal, which are applied to the decoding circuits 262, 264 and 266, respectively.

[0059] The decoding circuits 254, 262, 264 and 266 decode the encoded data inputted thereto, respectively. The output of the decoding circuit 254 is the LL signal. The SD D/A conversion circuit 268 converts the output of the decoding circuit 254 to an analog signal. The output of the SD D/A conversion circuit 268 is an analog video signal having the number of scan lines of 525 and the frame frequency of 30 Hz and it can be displayed as an image by an image display device of the ordinary resolution.

[0060] The reproduced LL signal and LH signal are combined at the vertical frequency by the band synthesization filters 270 and 272 and the number of pixels in the vertical direction is interpolated to two times. Similarly, the reproduced HL signal and HH signal are synthesized at the vertical frequency by the band synthesization filters 274 and 276 and the number of pixels in the vertical direction is interpolated to two times. The synthesized signals are combined at the horizontal frequency by the band synthesization filters 278 and 280 and the number of pixels in the horizontal direction is interpolated to two times.

[0061] By those synthesization processes, the digital high resolution video signal having the number of scan lines of 1,050 and the frame frequency of 30 Hz is reproduced. The HD D/A conversion circuit 282 converts

the reproduced digital HD signal to an analog signal.

[0062] In the decoding apparatus shown in Fig. 10, in the no key state, the decryption circuit 256 outputs a quite unstable data pattern so that the output of the HD D/A conversion circuit 282 is also unstable and an unstable pattern such as a noise image is displayed on the screen of the display device such as CRT.

[0063] Alternatively, the image of the low resolution or a still image may be displayed on the high resolution monitor screen in the no key state. Figs. 12 and 13 show portions of block diagrams of such modified decoding apparatus. The like elements to those of Fig. 10 are designated by the like numerals.

[0064] In Fig. 12, an SD/HD conversion circuit 284 for converting the output of the decoding circuit 254 to the HD signal and a selection switch for selecting the output of the SD/HD conversion circuit 284 or the synthesized output by the band synthesization filters 278 and 280 and supplying it to the HD D/A conversion circuit 282 are provided. The SD/HD conversion circuit 284 is identical to the SD/HD conversion circuit 54 of Fig. 6. The switch 286 is normally connected to synthezied output of the band synthesization filters 278 and 280, and when no key state is detected by the decryption circuit, it is switched to the output of the SD/HD conversion circuit 284 by the detection output. Thus, in the no key state, the image can be displayed by the high resolution monitor although the quality of the image is not sufficient for the high resolution monitor.

[0065] When the encryption key signal may not be inputted to the decryption circuit 256', it may be possible that the output of the encryption key output circuit 258 is forcibly stopped or the encryption key output circuit 258 itself is not present.

[0066] For the configuration shown in Fig. 12, the high frequency data of the band synthesization filters 270-280 may be reset by the detection output of the decryption circuit 256' to attain the same effect.

[0067] In Fig. 13, a switch 282 is provided between the synthesized output by the band synthesization filters 278 and 280 and the HD D/A conversion circuit 282 so that in the no key state, a predetermined level is inputted to the HD D/A conversion circuit 282. The switch 288 normally selects the synthesized output by the band synthesization filters 278 and 280, and when the no key state is detected by the decryption circuit 256, it is switched to the predetermined level input by the detection output. In this manner, when the correct encryption key is present, the high resolution video signal is outputted, but in the no key state, the predetermined level signal is outputted and the image corresponding to the predetermined level is displayed on the monitor screen.

[0068] When the encryption key signal is not inputted to the decryption circuit 256', it may be possible that the output of the encryption key output circuit is forcibly stopped or the encryption key output circuit 258 itself is not present.

[0069] For the configuration shown in Fig. 13, the switch 288 may not be provided and the output of the HD D/A conversion circuit 282 may be forced to a constant level (for example, zero output) in accordance with the detection output of the no key state by the decryption circuit 44.

[0070] In Figs. 12 and 13, the no key state is detected by the decryption circuit 256 although it may be detected by an error detection code or error correction process.

[0071] Embodiments of the encoding circuit and the decoding circuit used in the respective embodiments are now explained.

[0072] Fig. 14 shows a block diagram of a specific embodiment of the encoding circuit.

[0073] The encoding circuit shown in Fig. 14 comprises a blocking circuit 301, a DCT circuit 302, a quantization circuit 303, a variable length encoding circuit (VLC) 304, a motion compensation circuit 305, a motion vector detection circuit 306, a rate control circuit 307, a local decoding circuit 308 and a buffer memory 309.

[0074] In Fig. 14, image data to be encoded is grouped into 8 x 8 pixel blocks by the block forming circuit 301 and they are supplied to the DCT (discrete cosine transform) circuit 302 through the switch 310.

[0075] The switch 310 is periodically (for example, for each frame or every several fields) switched to a terminal a to prevent erroneous propagation.

[0076] Namely, when it is connected to the terminal a, an intra-frame or intra-field encoding (intra mode) is conducted.

[0077] In the intra mode, it is DCT-transformed by the DCT circuit 302 and the resulting DCT coefficient is quantized by the quantization circuit 303 and further encoded by the variable length encoding circuit 304 and temporarily stored in the buffer 309.

[0078] On the other hand, in other than the intra mode, the switch 310 is connected to a terminal b to conduct the motion compensated prediction encoding.

[0079] Numerals 311 and 312 denote a de-quantization circuit and a de-DCT circuit which constitute the local decoding circuit 308. The data quantized by the quantization circuit 303 is restored to the original image data by the local decoding circuit 308.

[0080] Numeral 313 denotes an adder, numeral 314 denotes a switch which is closed in other than the intra mode, and numeral 316 denotes a subtractor.

[0081] The locally decoded image data refers the motion vector detected by the motion vector detection circuit 306 to output the corresponding block of the predetermined frame (preceding frame, succeeding frame or interpolated frame).

[0082] The output of the motion compensation circuit 305 is subtracted by the input image data by the subtractor 316 to produce a difference.

[0083] The difference is encoded by the DCT circuit 302, the quantization circuit 303 and the variable length encoding circuit 304 and it is stored in the buffer 309.

[0084] The motion vector detection circuit 306 compares the frame data to be encoded with the predeter-

mined reference frame data to produce the motion vector, and the output of the motion vector detection circuit 306 is supplied to the motion compensation circuit 305 to specify the block to be outputted by the motion compensation circuit 305.

[0085] The rate control circuit 307 controls the quantity of encoding by switching the quantization step of the quantization circuit 303 in accordance with an occupation rate of the encoded data in the buffer 309.

[0086] Finally, the motion vector data detected by the motion vector detection circuit 306, an encoding identification code for identifying the intra mode and quantization step data indicating the quantization step are added by an adding circuit 315 and it is outputted as the encoded data.

[0087] Fig. 15 shows a specific block diagram of the decoding circuit.

[0088] The decoding circuit basically operates in the reverse manner to the encoding circuit shown in Fig. 14.

[0089] The decoding circuit shown in Fig. 15 comprises an input buffer memory 401, a variable length decoding circuit 402, a de-quantization circuit 403, a de-DCT circuit 404, a motion compensation circuit 405 and an output buffer memory 406.

[0090] The encoded data sequentially read from the input buffer memory 401 is processed by the variable length decoding circuit 402, the de-quantization circuit 403 and the de-DCT circuit 404 and converted to the space area data.

[0091] The quantization step of the de-quantization circuit 403 is determined by the quantization step data which is transmitted along with the encoded data.

[0092] Numeral 407 denotes an adder for adding the output of the de-DCT circuit 404 to the difference outputted from the motion compensation circuit 405, and numeral 408 denotes a switch for selecting the output of the de-DCT circuit 404 or the output of the adder 407.

[0093] The switch 408 is connected to the terminal a in the intra mode by the encoding identification code detected by the data detection circuit, not shown, and connected to the terminal b in other mode.

[0094] The decoded data is temporarily stored in the output buffer memory 406 and restored to the original space arrangement and outputted as one-frame or one-field image data.

[0095] As will be readily understood from the above description, in accordance with the present embodiment, the high resolution video signal is not reproduced for those who do not have the encryption key and the reproduction of only the low resolution video signal is permitted. The charges to the users may be discriminated between the display device of the low resolution and the display device of the high resolution of the same content.

[0096] The present invention may be implemented in other various forms.

[0097] For example, while the image signal is divided into four frequency bands in the second embodiment, the present invention is not limited thereto.

[0098] In other words, the foregoing description of the embodiments has been given for illustrative purpose only and not to be construed as imposing limitation in every respect.

[0099] The scope of the invention is, therefore, to be determined solely by the following claims and not limited by the text of the specification and alterations made within the scope equivalent to the scope of the claims fall within the scope of the invention.

Claims

1. An image processing apparatus comprising:

   a) input means for inputting an image signal (210);
   b) separation means (214 to 224) for separating said image signal into a low frequency component and a high frequency component in each of horizontal and vertical directions and for producing spatial frequency bands (LL, LH, HL, HH) from said image signal;
   c) encoding means (226 to 232) for high-efficiency encoding the spatial frequency bands (LH, HL, HH) including a highest frequency component and for high-efficiency encoding the spatial frequency band (LL) including a lowest frequency component; and
   d) encryption means (236) for encrypting only the encoded spatial frequency bands including the highest frequency component using an encryption key in accordance with a predetermined encryption algorithm.

2. An apparatus according to claim 1, wherein said separation means is operable to produce a first spatial frequency band (LL) including the low frequency component of the horizontal direction and the low frequency component of the vertical direction, a second spatial frequency band (LH) including the low frequency component of the horizontal direction and the high frequency component of the vertical direction, a third spatial frequency band (HL) including the high frequency component of the horizontal direction and the low frequency component of the vertical direction, and a fourth spatial frequency band (HH) including the high frequency component of the horizontal direction and the high frequency component of the vertical direction.

3. An apparatus according to claim 1 or 2, wherein said encoding means is operable to encode the spatial frequency bands using variable length encoders.

4. An apparatus according to any of claims 1 to 3, fur-

ther comprising:

multiplexing means (234) for multiplexing the spatial frequency bands to be encrypted, and wherein said encryption means is operable to encrypt an output of said multiplexing means.

5. An apparatus according to any of claims 1 to 4, further comprising second multiplexing means (240) for multiplexing the encoded spatial frequency bands encrypted by said encryption means and the encoded spatial frequency band not encrypted by said encryption means.

6. An image processing apparatus comprising:

a) input means (250) for inputting spatial frequency bands (LH, HL, HH) including a highest frequency component and spatial frequency band (LL) including a lowest frequency component, the spatial frequency bands including the highest frequency component are encrypted;
b) decryption means (256 or 256') for decrypting the spatial frequency bands including the highest frequency component using a decryption key in accordance with a predetermined decryption algorithm; and
c) decoding means (254 to 266) for decoding the decrypted spatial frequency bands including the highest frequency component and for decoding the spatial frequency band including the lowest frequency component.

7. An apparatus according to claim 6, wherein said input means inputs a first spatial frequency band (LL) including the low frequency component of the horizontal direction and the low frequency component of the vertical direction, a second spatial frequency band (LH) including the low frequency component in the horizontal direction and the high frequency component in the vertical direction, a third spatial frequency band (HL) including the high frequency component of the horizontal direction and the low frequency component of the vertical direction and a fourth spatial frequency band (HH) including the high frequency component of the horizontal direction and the high frequency component in the vertical direction.

8. An apparatus according to any of claims 6 and 7, further comprising:

synthesizing means (270 to 280) for synthesizing the decrypted spatial frequency bands with other spatial frequency bands.

9. An apparatus according to any of claims 6 to 8, further comprising demultiplexing means (260) for demultiplexing the decrypted spatial frequency bands, and said decoding means is operable to decode an output of said demultiplexing means.

10. An apparatus according to any of claims 6 to 9, wherein said decoding means is operable to decode the spatial frequency bands using variable length decoders.

11. An apparatus according to any of claims 6 to 10, further comprising inhibiting means (286) operable to inhibit an output of said decryption means when said decryption means cannot decrypt the encrypted spatial frequency band.

12. An apparatus according to any of claims 6 to 11, further comprising means (288) for producing a predetermined signal in lieu of the encrypted spatial frequency band when said decryption means cannot decrypt the encrypted spatial frequency band.

13. An image processing method comprising:

a) an input step of inputting an image signal (210);
b) a separation step of separating said image signal into a low frequency component and a high frequency component in each of horizontal and vertical directions and of producing spatial frequency bands (LL, LH, HL, HH) from said image signal;
c) an encoding step of high-efficiency encoding the spatial frequency bands (LH, HL, HH) including a highest frequency component and of high-efficiency encoding the spatial frequency band (LL) including a lowest frequency component; and
d) an encryption step of encrypting only the encoded spatial frequency bands including the highest frequency component using an encryption key in accordance with a predetermined encryption algorithm.

14. A method as claimed in claim 13, wherein said separation step produces a first spatial frequency band (LL) including the low frequency component of the horizontal direction and the low frequency component of the vertical direction, a second spatial frequency band (LH) including the low frequency component of the horizontal direction and the high frequency component of the vertical direction, a third spatial frequency band (HL) including the high frequency component of the horizontal direction and the low frequency component of the vertical direction, and a fourth spatial frequency band (HH) including the high frequency component of the horizontal direction and the high frequency component of the vertical direction.

15. A method as claimed in any of claims 13 and 14 wherein said encoding step encode the spatial frequency bands using variable length encoders.

16. A method as claimed in any of claims 13 to 15, further comprising:

a multiplexing step of multiplexing the spatial frequency bands to be encrypted, and
wherein said encryption step encrypts an output of said multiplexing step.

17. A method as claimed in any of claims 13 to 16, further comprising a second multiplexing step of multiplexing the encoded spatial frequency bands encrypted by said encryption step and the encoded spatial frequency band not encrypted by said encryption step.

18. An image processing method comprising:

a) an input step inputting spatial frequency bands (LH, HL, HH) including a highest frequency component and spatial frequency band (LL) including a lowest frequency component, the spatial frequency bands including the highest frequency component are encrypted;
b) a decryption step of decrypting the spatial frequency bands including the highest frequency component using a decryption key in accordance with a predetermined decryption algorithm; and
c) a decoding step of decoding the decrypted spatial frequency bands including the highest frequency component and of decoding the spatial frequency band including the lowest frequency component.

19. A method as claimed in claim 18, wherein said input step inputs a first spatial frequency band (LL) including the low frequency component of the horizontal direction and the low frequency component of the vertical direction, a second spatial frequency band (LH) including the low frequency component of the horizontal direction and the high frequency component of the vertical direction, a third spatial frequency band (HL) including the high frequency component of the horizontal direction and the low frequency component of the vertical direction and a fourth spatial frequency band (HH) including the high frequency component of the horizontal direction and the high frequency component of the vertical direction.

20. A method as claimed in any of claims 18 and 19, further comprising:

a synthesizing step of synthesizing the decrypted spatial frequency bands with other spatial frequency bands.

21. A method as claimed in any of claims 18 to 20, further comprising a demultiplexing step of demultiplexing the decrypted spatial frequency bands, and said decoding means is operable to decode an output of said demultiplexing means.

22. A method as claimed in any of claims 18 to 21, wherein said decoding means is operable to decode the spatial frequency bands using variable length decoders .

23. A method as claimed in any of claims 18 to 22, further comprising an inhibiting step of inhibiting an output of said decryption step when said decryption step cannot decrypt the encrypted spatial frequency band.

24. A method as claimed in any of claims 18 to 23, further comprising a step of producing a predetermined signal in lieu of the encrypted spatial frequency band when said decryption step cannot decrypt the encrypted spatial frequency band.

Patentansprüche

1. Vorrichtung zur Bildverarbeitung, mit:

a) einem Eingabemittel zur Eingeben eines Bildsignals (210);
b) einem Trennmittel (214 bis 224) zum Trennen des Bildsignals in eine niederfrequente Komponente und in eine hochfrequente Komponente sowohl in Horizontal- als auch in Vertikalrichtung, um aus dem Bildsignal ein Ortsfrequenzband (LL, LH, HL, HH) zu erzeugen;
c) einem Codiermittel (226 bis 232) zum hocheffizienten Codieren der eine Höchstfrequenzkomponente enthaltenden Ortsfrequenzbänder (LH, HL, HH) und des eine Niedrigstfrequenzkomponente enthaltenden Ortsfrequenzbandes (LL); und mit
d) einem Verschlüsselungsmittel (236) zum Verschlüsseln nur der die Höchstfrequenzkomponente enthaltenden codierten Ortsfrequenzbänder unter Verwendung eines Schlüssels gemäß einem vorbestimmten Verschlüsselungsalgorithmus.

2. Vorrichtung nach Anspruch 1, bei der das Trennmittel betriebsbereit ist zum Erzeugen eines ersten Ortsfrequenzbandes (LL) mit der Niederfrequenzkomponente der Horizontalrichtung unter der Niederfrequenzkomponente der Vertikalrichtung, eines zweiten Ortsfrequenzbandes (LH) mit der Nie-

derfrequenzkomponente der Horizontalrichtung und der Hochfrequenzkomponente der Vertikalrichtung, eines dritten Ortsfrequenzbandes (HL) mit der Hochfrequenzkomponente der Horizontalrichtung und der Niederfrequenzkomponente der Vertikalrichtung, und zum Erzeugen eines vierten Ortsfrequenzbandes (HH) mit der Hochfrequenzkomponente der Horizontalrichtung und der Hochfrequenzkomponente der Vertikalrichtung.

3. Vorrichtung nach Anspruch 1 oder 2, bei der das Codiermittel betriebsbereit ist, die Ortsfrequenzbänder unter Verwendung eines längenvariabel codierenden Codierers zu codieren.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, die des weiteren ausgestattet ist mit:

einem Multiplexmittel (234) zum Multiplexieren der zu verschlüsselnden Ortsfrequenzbänder,

wobei das Verschlüsselungsmittel betriebsbereit ist, ein Ausgangssignal des Multiplexmittels zu verschlüsseln.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, die des weiteren über ein zweites Multiplexmittel (240) verfügt, um die vom Verschlüsselungsmittel verschlüsselten codierten Ortsfrequenzbänder und das nicht vom Verschlüsselungsmittel verschlüsselte codierte Ortsfrequenzband zu multiplexieren.

6. Vorrichtung zur Bildverarbeitung; mit:

a) einem Eingabemittel (25) zur Eingabe von Ortsfrequenzbändern (LH, HL, HH) mit einer Höchstfrequenzkomponente und einem Ortsfrequenzband (LL) mit einer Niedrigstfrequenzkomponente, wobei die die Höchstfrequenzkomponente enthaltenden Ortsfrequenzbänder verschlüsselt sind;
b) einem Verschlüsselungsmittel (256 oder 256') zum Verschlüsseln der Ortsfrequenzbänder, die die Höchstfrequenzkomponente enthalten, unter Verwendung eines Schlüssels gemäß einem vorbestimmten Verschlüsselungsalgorithmus; und mit
c) einem Codiermittel (254 bis 266) zum Decodieren der verschlüsselten Ortsfrequenzbänder, die die Höchstfrequenzkomponente enthalten, und zum Decodieren des Ortsfrequenzbandes, das die Niedrigstfrequenzkomponente enthält.

7. Vorrichtung nach Anspruch 6, bei der das Eingabemittel ein erstes Ortsfrequenzband (LL), das die Niederfrequenzkomponente der Horizontalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, ein zweites Ortsfrequenzband (LH), das die Niederfrequenzkomponente in Horizontalrichtung und die Hochfrequenzkomponente in Vertikalrichtung enthält, ein drittes Ortsfrequenzband (HL), das die Hochfrequenzkomponente der Horizontalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, und ein viertes Ortsfrequenzband (HH) eingibt, das die Hochfrequenzkomponente der Horizontalrichtung und die Hochfrequenzkomponente der Vertikalrichtung enthält.

8. Vorrichtung nach einem der der Ansprüche 6 bis 8, die des weiteren ausgestattet ist mit:

einem Synthetisiermittel (270 bis 280) zum Zusammensetzen der entschlüsselten Ortsfrequenzbänder mit anderen Ortsfrequenzbändern.

9. Vorrichtung nach einem der Ansprüche 6 bis 8, die des weiteren über ein Demultiplexmittel (260) verfügt, um die verschlüsselten Ortsfrequenzbänder zu demultiplexieren, und wobei das Decodiermittel betriebsbereit ist, ein Ausgangssignal vom Demultiplexmittel zu decodieren.

10. Vorrichtung nach einem der Ansprüche 6 bis 9, bei der das Decodiermittel betriebsbereit ist, die Ortsfrequenzbänder unter Verwendung von längenvariabel decodierenden Decodierern zu decodieren.

11. Vorrichtung nach einem der Ansprüche 6 bis 10, die des weiteren über ein Sperrmittel (286) verfügt, das betriebsbereit ist zum Sperren eines Ausgangssignals vom Entschlüsselungsmittel, wenn das Entschlüsselungsmittel das verschlüsselte Ortsfrequenzband nicht entschlüsseln kann.

12. Vorrichtung nach einem der Ansprüche 6 bis 11, mit einem weiteren Mittel (288) zum Erzeugen eines vorbestimmten Signals anstelle des verschlüsselten Ortsfrequenzbandes, wenn das Verschlüsselungsmittel das verschlüsselte Ortsfrequenzband nicht entschlüsseln kann.

13. Verfahren zur Bildverarbeitung, mit den Verfahrensschritten:

a) Eingeben eines Bildsignals (210);
b) Trennen des Bildsignals in eine Niederfrequenzkomponente und eine Hochfrequenzkomponente jeweils in Horizontal- und Vertikalrichtung und Erzeugen von Ortsfrequenzbändern (LL, LH. HL, HH) aus dem Bildsignal;
c) hocheffizientes Codieren der Ortsfrequenzbänder (LH, HL, HH), die eine Höchstfrequenzkomponente enthalten, und des Ortsfrequenz-

bandes (LL), das eine Niedrigstfrequenzkomponente enthält; und

d) Verschlüsseln nur der codierten Ortfrequenzbänder, die die Höchstfrequenzkomponente enthalten, unter Verwendung eines Schlüssels gemäß einem vorbestimmten Verschlüsselungsalgorithmus.

14. Verfahren nach Anspruch 13, bei dem der Verfahrensschritt des Trennens ein erstes Ortsfrequenzband (LL), das die Niederfrequenzkomponente der Horizontalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, ein zweites Ortsfrequenzband (LH), das die Niederfrequenzkomponente der Horizontalrichtung und die Hochfrequenzkomponente der Vertikalrichtung enthält, ein drittes Ortsfrequenzband (HL), das die Hochfrequenzkomponente der Horizontalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, und ein viertes Ortsfrequenzband (HH) erzeugt, das die Hochfrequenzkomponente der Horizontalrichtung und die Hochfrequenzkomponente der Vertikalrichtung enthält.

15. Verfahren nach einem der Ansprüche 13 und 14, bei dem der Verfahrensschritt des Codierens die Ortsfrequenzbänder unter Verwendung eines längenvariabel codierenden Codierers codiert.

16. Verfahren nach einem der Ansprüche 13 bis 15, mit den weiteren Verfahrensschritten:

Multiplexieren der zu verschlüsselnden Ortsfrequenzbänder und

wobei der Verfahrensschritt des Verschlüsselns ein beim Multiplexieren abgegebenes Signal verschlüsselt.

17. Verfahren nach einem der Ansprüche 13 bis 16, mit dem weiteren Verfahrensschritt eines zweiten Multiplexierens der im Verfahrensschritt des Verschlüsselns verschlüsselten codierten Ortsfrequenzbänder und dem im Verfahrensschritt des Verschlüsselns nicht verschlüsselten codierten Ortsfrequenzband.

18. Verfahren zur Bildverarbeitung, mit den Verfahrensschritten:

a) Eingeben von eine Höchstfrequenzkomponente enthaltende Ortsfrequenzbändern (LH, HL, HH) und von einem eine Niedrigstfrequenzkomponente enthaltenden Ortsfrequenzband (LL), wobei die die Höchstfrequenzkomponente enthaltende Ortsfrequenzbänder verschlüsselt sind;

b) Entschlüsseln der Ortsfrequenzbänder, die die Höchstfrequenzkomponente enthalten, unter Verwendung eines Schlüssels gemäß einem vorbestimmten Entschlüsselungsalgorithmus; und

c) Decodieren der die Höchstfrequenzkomponente enthaltenden verschlüsselten Ortsfrequenzbänder und des die Niedrigstfrequenzkomponente enthaltenden Ortsfrequenzbandes.

19. Verfahren nach Anspruch 18, bei dem der Verfahrensschritt des Eingebens folgende Eingaben umfaßt: ein erstes Ortsfrequenzband (LL), das die Niederfrequenzkomponente der Horizontalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, ein zweites Ortsfrequenzband (LH), das die Niederfrequenzkomponente der Horizontalrichtung und die Hochfrequenzkomponente der Vertikalrichtung enthält, ein drittes Ortsfrequenzband (HL), das die Hochfrequenzkomponente der Vertikalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, und ein viertes Ortsfrequenzband (HH), das die Hochfrequenzkomponente der Horizontalrichtung und die Hochfrequenzkomponente der Vertikalrichtung enthält.

20. Verfahren nach einem der Ansprüche 18 und 19, mit dem weiteren Verfahrensschritt:

Synthetisieren der entschlüsselten Ortsfrequenzbänder mit anderen Ortsfrequenzbändern.

21. Verfahren nach einem der Ansprüche 18 bis 20, mit den weiteren Verfahrensschritt des Demultiplexierens der entschlüsselten Ortsfrequenzbänder, wobei das Decodiermittel betriebsbereit ist, das Ausgangssignal vom Demultiplexer zu decodieren.

22. Verfahren nach einem der Ansprüche 18 bis 21, bei dem das Decodiermittel betriebsbereit ist, die Ortsfrequenzbänder mit längenvariabel decodierenden Codierern zu decodieren.

23. Verfahren nach einem der Ansprüche 18 bis 22, mit dem weiteren Verfahrensschritt des Sperrens eines beim Entschlüsseln ausgegebenen Signals, wenn der Verfahrensschritt des Entschlüsselns das verschlüsselte Ortsfrequenzband nicht entschlüsseln kann.

24. Verfahren nach einem der Ansprüche 18 bis 23, mit dem weiteren Verfahrensschritt des Erzeugens eines vorbestimmten Signals anstelle des verschlüsselten Ortsfrequenzbandes, wenn der Verfahrensschritt des Entschlüsselns das verschlüsselte Ortsfrequenzband nicht entschlüsseln kann.

Revendications

1. Appareil de traitement d'image, comprenant :

   a) un moyen d'entrée pour introduction d'un signal (210) d'image ;
   b) un moyen (214 à 224) de séparation pour séparer ledit signal d'image en une composante basse fréquence et une composante haute fréquence dans chacune de directions horizontale et verticale et pour produire des bandes (LL, LH, HL, HH) de fréquence spatiale à partir dudit signal d'image ;
   c) un moyen (226 à 232) de codage pour un codage de grande efficacité des bandes (LH, HL, HH) de fréquence spatiale comportant une composante de fréquence supérieure et pour un codage de grande efficacité de la bande (LL) de fréquence spatiale comportant une composante de fréquence inférieure ; et
   d) un moyen (236) de cryptage pour crypter uniquement les bandes codées de fréquence spatiale comportant la composante de fréquence supérieure en utilisant une clé de cryptage en fonction d'un algorithme prédéterminé de cryptage.

2. Appareil selon la revendication 1, dans lequel ledit moyen de séparation peut fonctionner pour produire une première bande (LL) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, une deuxième bande (LH) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante haute fréquence de la direction verticale, une troisième bande (HL) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, et une quatrième bande (HH) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante haute fréquence de la direction verticale.

3. Appareil selon la revendication 1 ou 2, dans lequel ledit moyen de codage peut fonctionner pour coder les bandes de fréquence spatiale en utilisant des codeurs de longueur variable.

4. Appareil selon l'une quelconque des revendications 1 à 3, comprenant en outre :

   un moyen (234) de multiplexage pour multiplexer les bandes de fréquence spatiale à crypter,
   et dans lequel ledit moyen de cryptage peut fonctionner pour crypter une sortie dudit moyen de multiplexage.

5. Appareil selon l'une quelconque des revendications 1 à 4, comprenant en outre un deuxième moyen (240) de multiplexage pour multiplexer les bandes codées de fréquence spatiale cryptées par ledit moyen de cryptage et la bande codée de fréquence spatiale non cryptée par ledit moyen de cryptage.

6. Appareil de traitement d'image, comprenant :

   a) un moyen (250) d'entrée pour introduction de bandes (LH, HL, HH) de fréquence spatiale comportant une composante de fréquence supérieure et une bande (LL) de fréquence spatiale comportant une composante de fréquence inférieure, les bandes de fréquence spatiale comportant la composante de fréquence supérieure étant cryptées ;
   b) un moyen (256 ou 256') de décryptage pour décrypter les bandes de fréquence spatiale comportant la composante de fréquence supérieure en utilisant une clé de décryptage en fonction d'un algorithme prédéterminé de décryptage ; et
   c) un moyen (254 à 266) de décodage pour décoder les bandes décryptées de fréquence spatiale comportant la composante de fréquence supérieure et pour décoder la bande de fréquence spatiale comportant la composante de fréquence inférieure.

7. Appareil selon la revendication 6, dans lequel ledit moyen d'entrée introduit une première bande (LL) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, une deuxième bande (LH) de fréquence spatiale comportant la composante basse fréquence dans la direction horizontale et la composante haute fréquence dans la direction verticale, une troisième bande (HL) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante basse fréquence de la direction verticale et une quatrième bande (HH) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante haute fréquence dans la direction verticale.

8. Appareil selon l'une quelconque des revendications 6 et 7, comprenant en outre :

   un moyen (270 à 280) de synthèse pour synthétiser les bandes décryptées de fréquence spatiale avec d'autres bandes de fréquence spatiale.

9. Appareil selon l'une quelconque des revendications

6 à 8, comprenant en outre un moyen (260) de démultiplexage pour démultiplexer les bandes décryptées de fréquence spatiale, et ledit moyen de décodage pouvant fonctionner pour décoder une sortie dudit moyen de démultiplexage.

10. Appareil selon l'une quelconque des revendications 6 à 9, dans lequel ledit moyen de décodage peut fonctionner pour décoder les bandes de fréquence spatiale en utilisant des décodeurs de longueur variable.

11. Appareil selon l'une quelconque des revendications 6 à 10, comprenant en outre un moyen (286) d'invalidation pouvant fonctionner pour invalider une sortie dudit moyen de décryptage lorsque ledit moyen de décryptage ne peut pas décrypter la bande cryptée de fréquence spatiale.

12. Appareil selon l'une quelconque des revendications 6 à 11, comprenant en outre un moyen (288) pour produire un signal prédéterminé au lieu de la bande cryptée de fréquence spatiale lorsque ledit moyen de décryptage ne peut pas décrypter la bande cryptée de fréquence spatiale.

13. Procédé de traitement d'image, comprenant :

a) une étape d'entrée, d'introduction d'un signal (210) d'image ;
b) une étape de séparation, de séparation dudit signal d'image en une composante basse fréquence et une composante haute fréquence dans chacune de directions horizontale et verticale et de production de bandes (LL, LH, HL, HH) de fréquence spatiale à partir dudit signal d'image ;
c) une étape de codage, de codage de grande efficacité des bandes (LH, HL, HH) de fréquence spatiale comportant une composante de fréquence supérieure et de codage de grande efficacité de la bande (LL) de fréquence spatiale comportant une composante de fréquence inférieure ; et
d) une étape de cryptage, de cryptage uniquement des bandes codées de fréquence spatiale comportant la composante de fréquence supérieure en utilisant une clé de cryptage en fonction d'un algorithme prédéterminé de cryptage.

14. Procédé selon la revendication 13, dans lequel ladite étape de séparation produit une première bande (LL) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, une deuxième bande (LH) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante haute fréquence de la direction verticale, une troisième bande (HL) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, et une quatrième bande (HH) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante haute fréquence de la direction verticale.

15. Procédé selon l'une quelconque des revendications 13 et 14, dans lequel ladite étape de codage code les bandes de fréquence spatiale en utilisant des codeurs de longueur variable.

16. Procédé selon l'une quelconque des revendications 13 à 15, comprenant en outre :

une étape de multiplexage, de multiplexage des bandes de fréquence spatiale à crypter, et dans lequel ladite étape de cryptage crypte une sortie de ladite étape de multiplexage.

17. Procédé selon l'une quelconque des revendications 13 à 16, comprenant en outre une deuxième étape de multiplexage, de multiplexage des bandes codées de fréquence spatiale cryptées par ladite étape de cryptage et de la bande codée de fréquence spatiale non cryptée par ladite étape de cryptage.

18. Procédé de traitement d'image, comprenant :

a) une étape d'entrée introduisant des bandes (LH, HL, HH) de fréquence spatiale comportant une composante de fréquence supérieure et une bande (LL) de fréquence spatiale comportant la composante de fréquence inférieure, les bandes de fréquence spatiale comportant la composante de fréquence supérieure étant cryptées ;
b) une étape de décryptage, de décryptage des bandes de fréquence spatiale comportant la composante de fréquence supérieure en utilisant une clé de décryptage en fonction d'un algorithme prédéterminé de décryptage ; et
c) une étape de décodage, de décodage des bandes décryptées de fréquence spatiale comportant la composante de fréquence supérieure et de décodage de la bande de fréquence spatiale comportant la composante de fréquence inférieure.

19. Procédé selon la revendication 18, dans lequel ladite étape d'entrée introduit une première bande (LL) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, une deuxième bande (LH) de fréquence spatiale comportant la composante basse fréquen-

ce de la direction horizontale et la composante haute fréquence de la direction verticale, une troisième bande (HL) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante basse fréquence de la direction verticale et une quatrième bande (HH) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante haute fréquence de la direction verticale.

20. Procédé selon l'une quelconque des revendications 18 et 19, comprenant en outre :

une étape de synthèse, de synthèse des bandes décryptées de fréquence spatiale avec d'autres bandes de fréquence spatiale.

21. Procédé selon l'une quelconque des revendications 18 à 20, comprenant en outre une étape de démultiplexage, de démultiplexage des bandes décryptées de fréquence spatiale, et ledit moyen de décodage peut fonctionner pour décoder une sortie dudit moyen de démultiplexage.

22. Procédé selon l'une quelconque des revendications 18 à 21, dans lequel ledit moyen de décodage peut fonctionner pour décoder les bandes de fréquence spatiale en utilisant des décodeurs de longueur variable.

23. Procédé selon l'une quelconque des revendications 18 à 22, comprenant en outre une étape d'invalidation, d'invalidation d'une sortie de ladite étape de décryptage lorsque ladite étape de décryptage ne peut pas décrypter la bande cryptée de fréquence spatiale.

24. Procédé selon l'une quelconque des revendications 18 à 23, comprenant en outre une étape de production d'un signal prédéterminé au lieu de la bande cryptée de fréquence spatiale lorsque ladite étape de décryptage ne peut pas décrypter la bande cryptée de fréquence spatiale.

FIG. 1

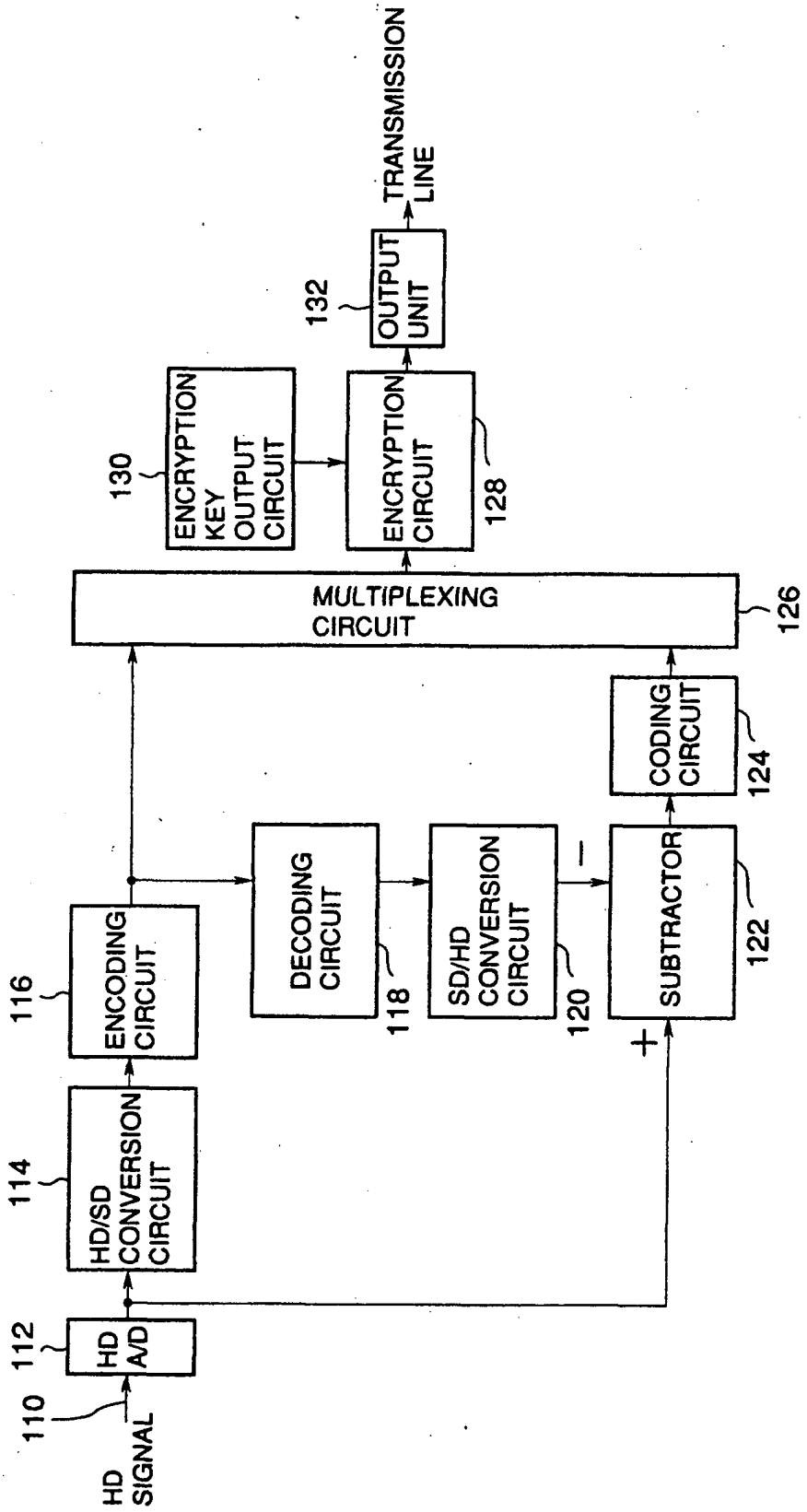

HD SIGNAL
110
HD A/D
112
HD/SD CONVERSION CIRCUIT
114
ENCODING CIRCUIT
116
DECODING CIRCUIT
118
SD/HD CONVERSION CIRCUIT
120
SUBTRACTOR
122
CODING CIRCUIT
124
MULTIPLEXING CIRCUIT
126
ENCRYPTION CIRCUIT
128
ENCRYPTION KEY OUTPUT CIRCUIT
130
OUTPUT UNIT
132
TRANSMISSION LINE
+
−

FIG. 2

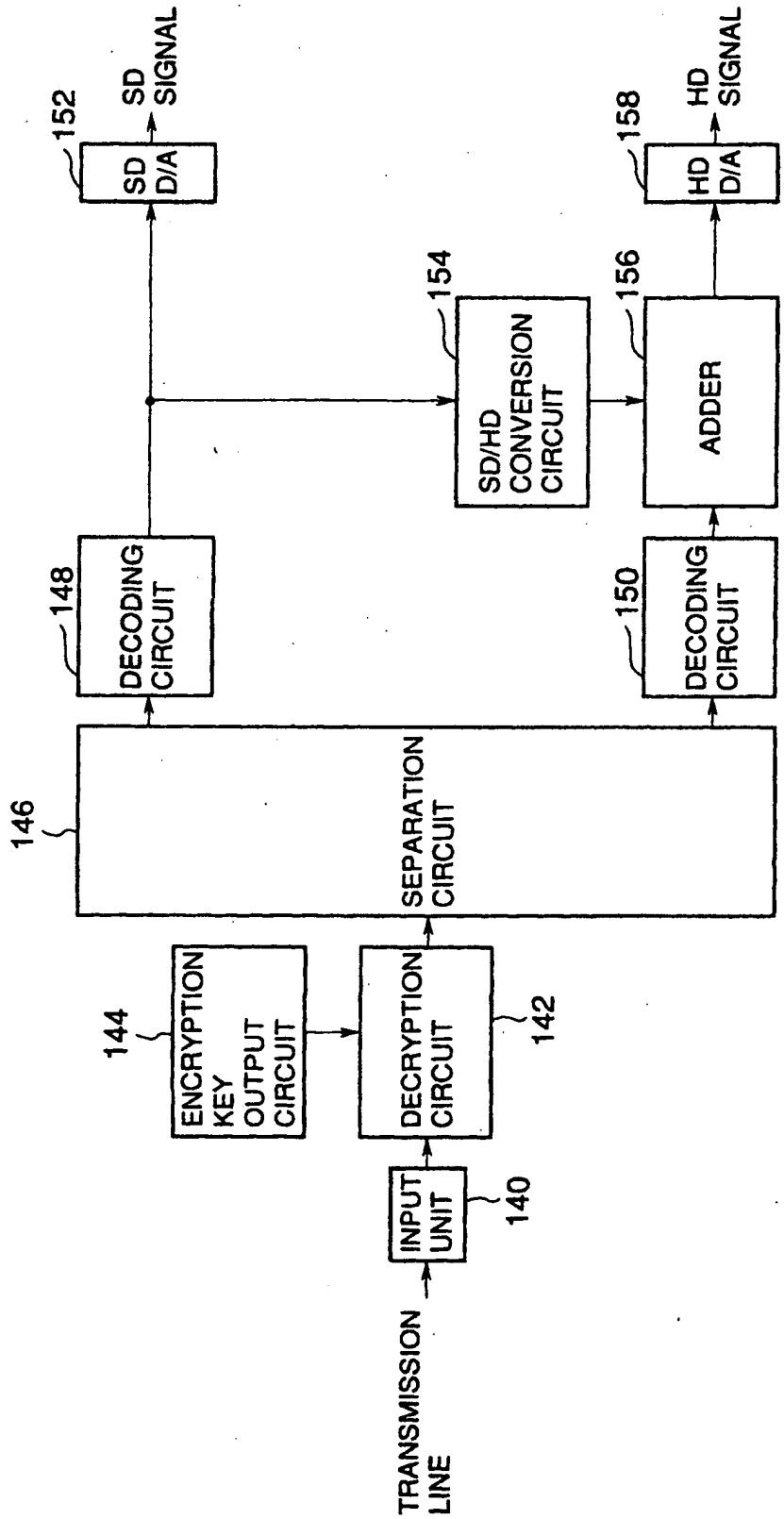

TRANSMISSION LINE
INPUT UNIT
140
DECRYPTION CIRCUIT
142
ENCRYPTION KEY OUTPUT CIRCUIT
144
SEPARATION CIRCUIT
146
DECODING CIRCUIT
148
DECODING CIRCUIT
150
SD/HD CONVERSION CIRCUIT
154
ADDER
156
SD D/A
152
SD SIGNAL
HD D/A
158
HD SIGNAL

FIG. 3

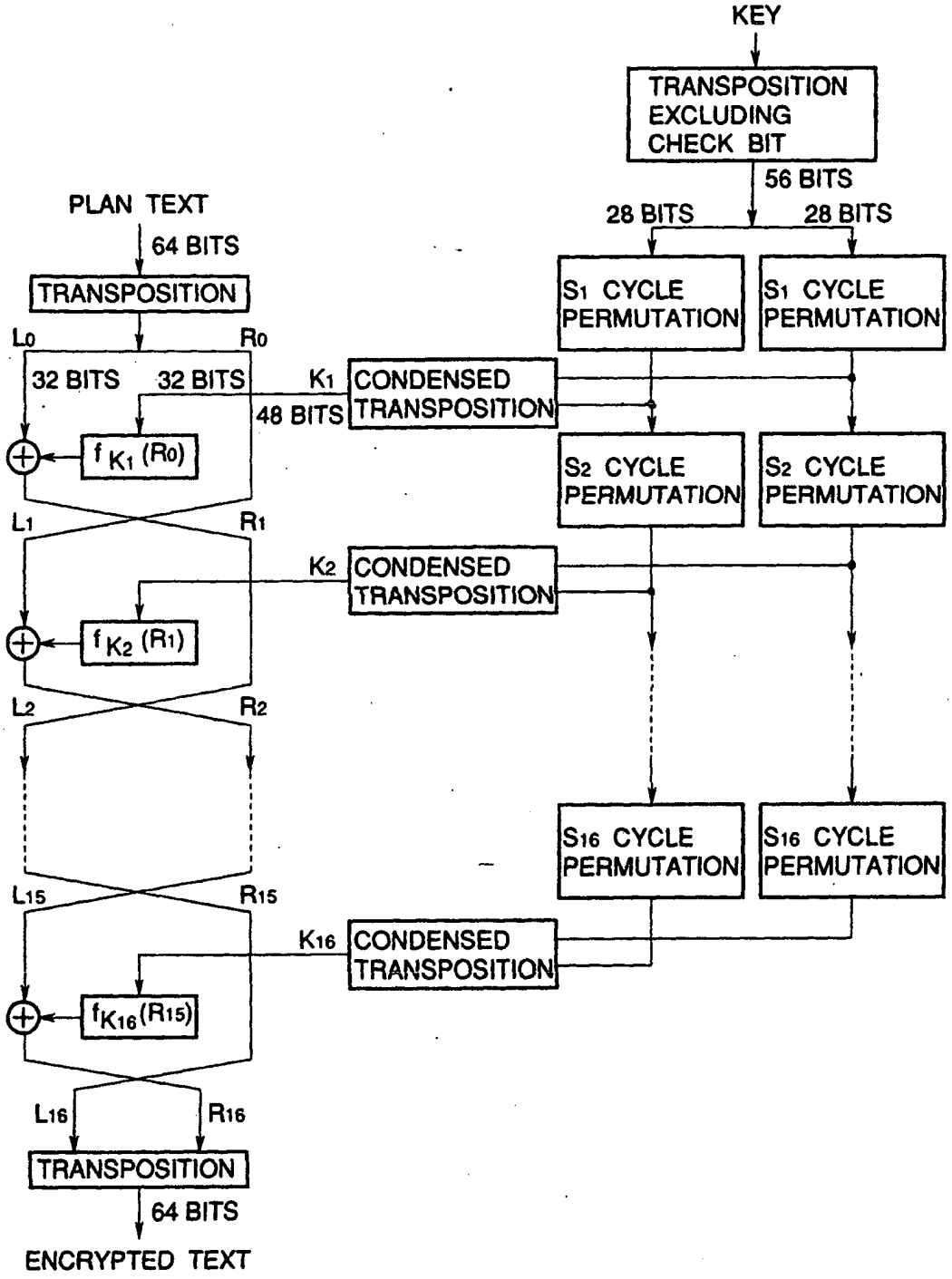

KEY
TRANSPOSITION EXCLUDING CHECK BIT
56 BITS
28 BITS
28 BITS
PLAN TEXT
64 BITS
TRANSPOSITION
L0
R0
32 BITS
32 BITS
K1
48 BITS
CONDENSED TRANSPOSITION
f K1 (R0)
S1 CYCLE PERMUTATION
S1 CYCLE PERMUTATION
S2 CYCLE PERMUTATION
S2 CYCLE PERMUTATION
L1
R1
K2
CONDENSED TRANSPOSITION
f K2 (R1)
L2
R2
S16 CYCLE PERMUTATION
S16 CYCLE PERMUTATION
L15
R15
K16
CONDENSED TRANSPOSITION
fK16(R15)
L16
R16
TRANSPOSITION
64 BITS
ENCRYPTED TEXT

FIG. 4

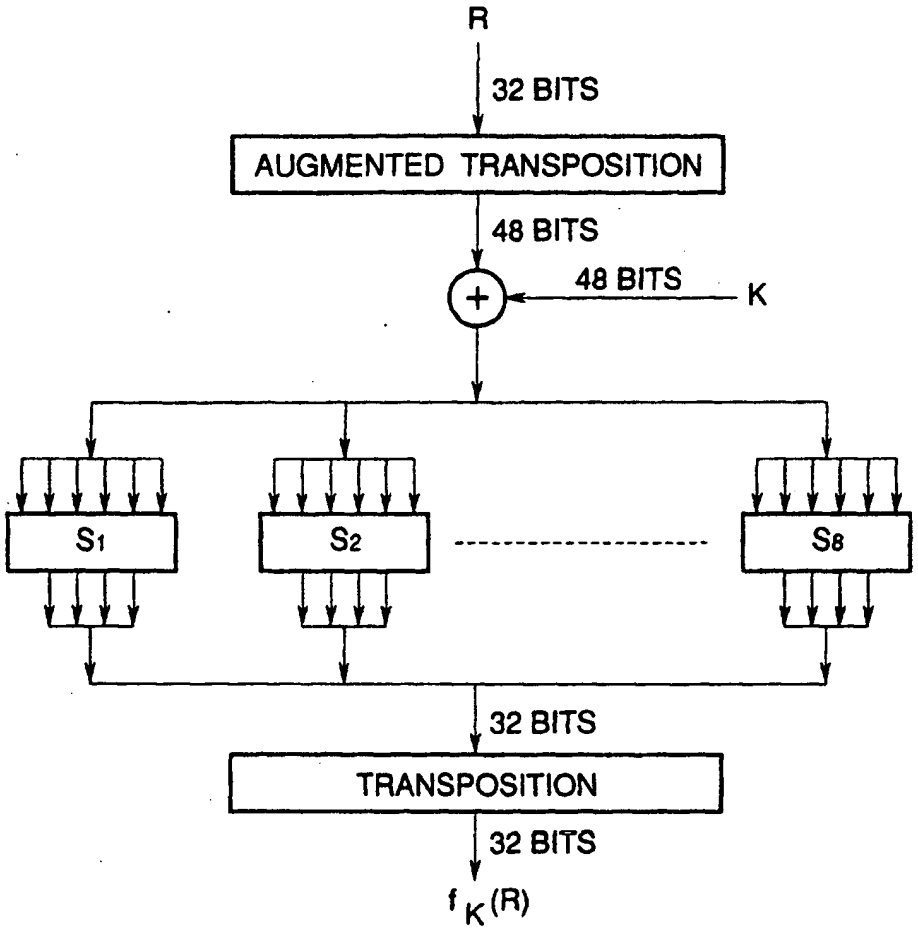

R
32 BITS
AUGMENTED TRANSPOSITION
48 BITS
48 BITS
K
S1
S2
S8
32 BITS
TRANSPOSITION
32 BITS
f K (R)

FIG. 5

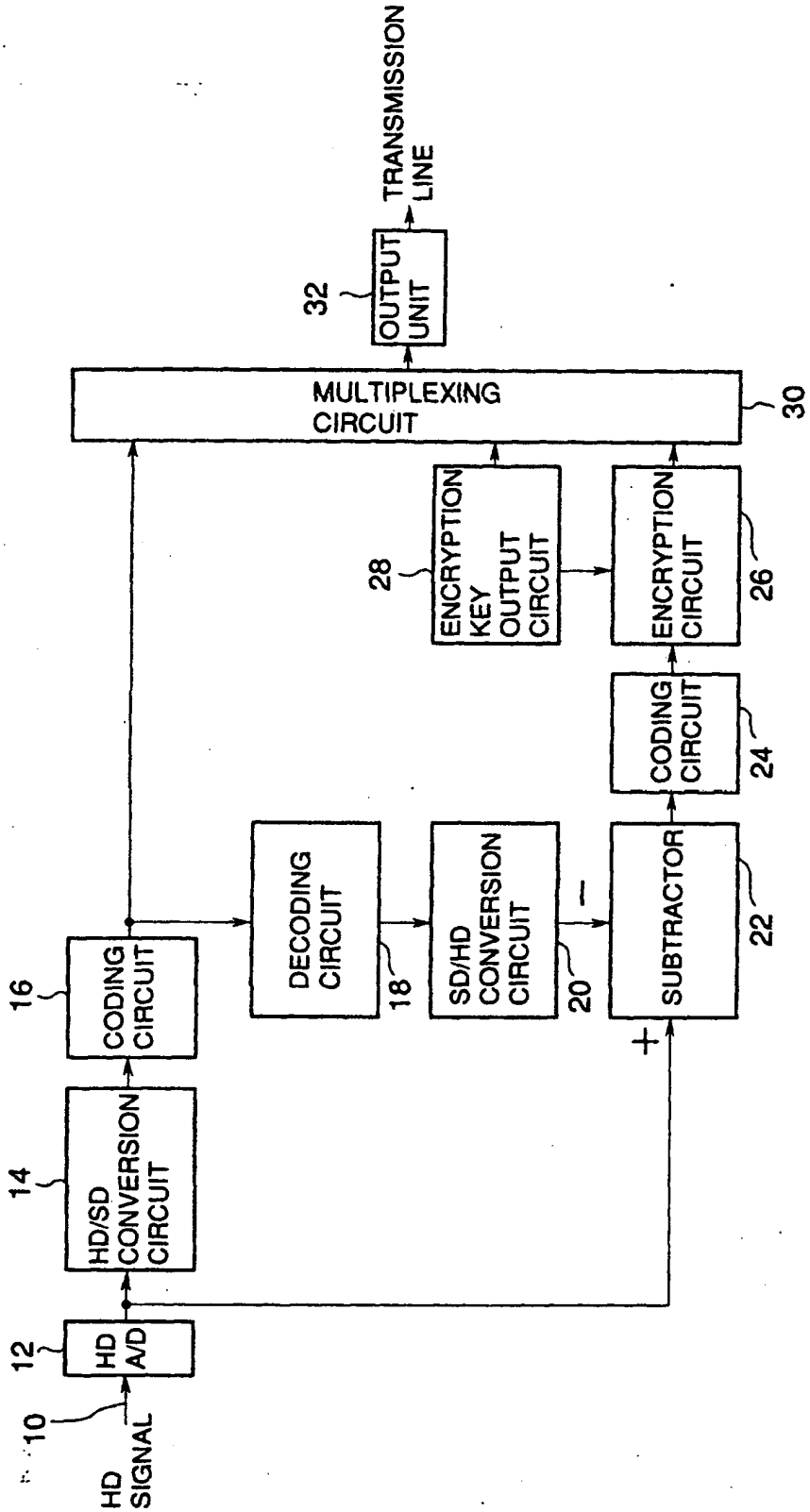

HD SIGNAL
10
HD A/D
12
HD/SD CONVERSION CIRCUIT
14
CODING CIRCUIT
16
DECODING CIRCUIT
18
SD/HD CONVERSION CIRCUIT
20
SUBTRACTOR
22
CODING CIRCUIT
24
ENCRYPTION CIRCUIT
26
ENCRYPTION KEY OUTPUT CIRCUIT
28
MULTIPLEXING CIRCUIT
30
OUTPUT UNIT
32
TRANSMISSION LINE
+
-

FIG. 6

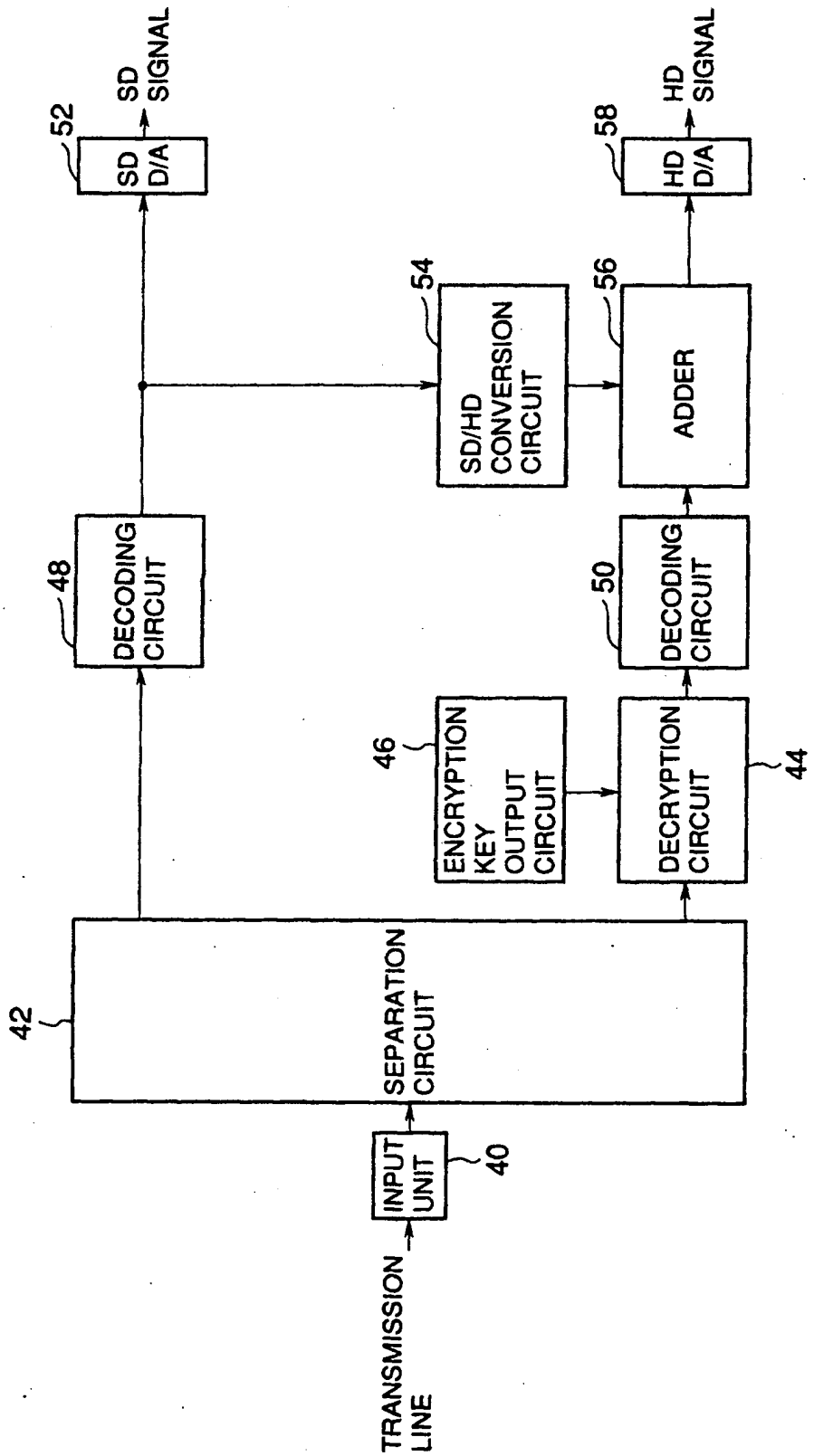

TRANSMISSION LINE
INPUT UNIT
40
SEPARATION CIRCUIT
42
DECODING CIRCUIT
48
SD D/A
52
SD SIGNAL
ENCRYPTION KEY OUTPUT CIRCUIT
46
DECRYPTION CIRCUIT
44
DECODING CIRCUIT
50
SD/HD CONVERSION CIRCUIT
54
ADDER
56
HD D/A
58
HD SIGNAL

FIG. 7

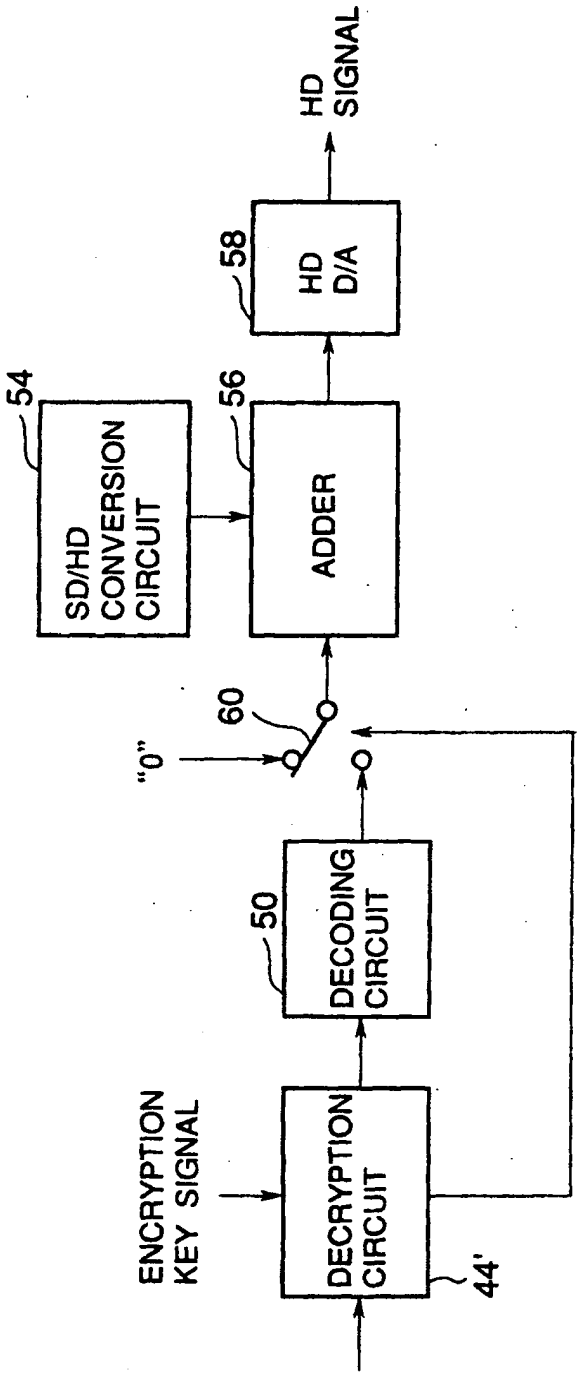

HD SIGNAL
58
HD D/A
54
SD/HD CONVERSION CIRCUIT
56
ADDER
60
"0"
50
DECODING CIRCUIT
ENCRYPTION KEY SIGNAL
DECRYPTION CIRCUIT
44'

FIG. 8

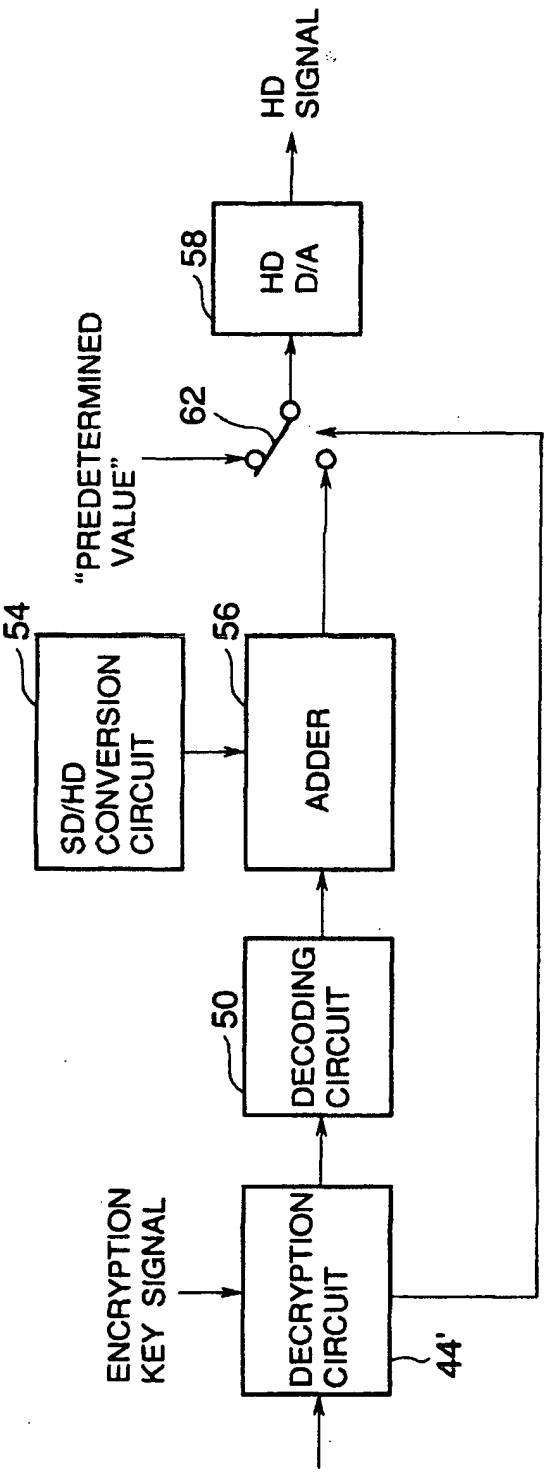

HD SIGNAL
58
HD D/A
62
"PREDETERMINED VALUE"
54
SD/HD CONVERSION CIRCUIT
56
ADDER
50
DECODING CIRCUIT
ENCRYPTION KEY SIGNAL
DECRYPTION CIRCUIT
44'

FIG. 9

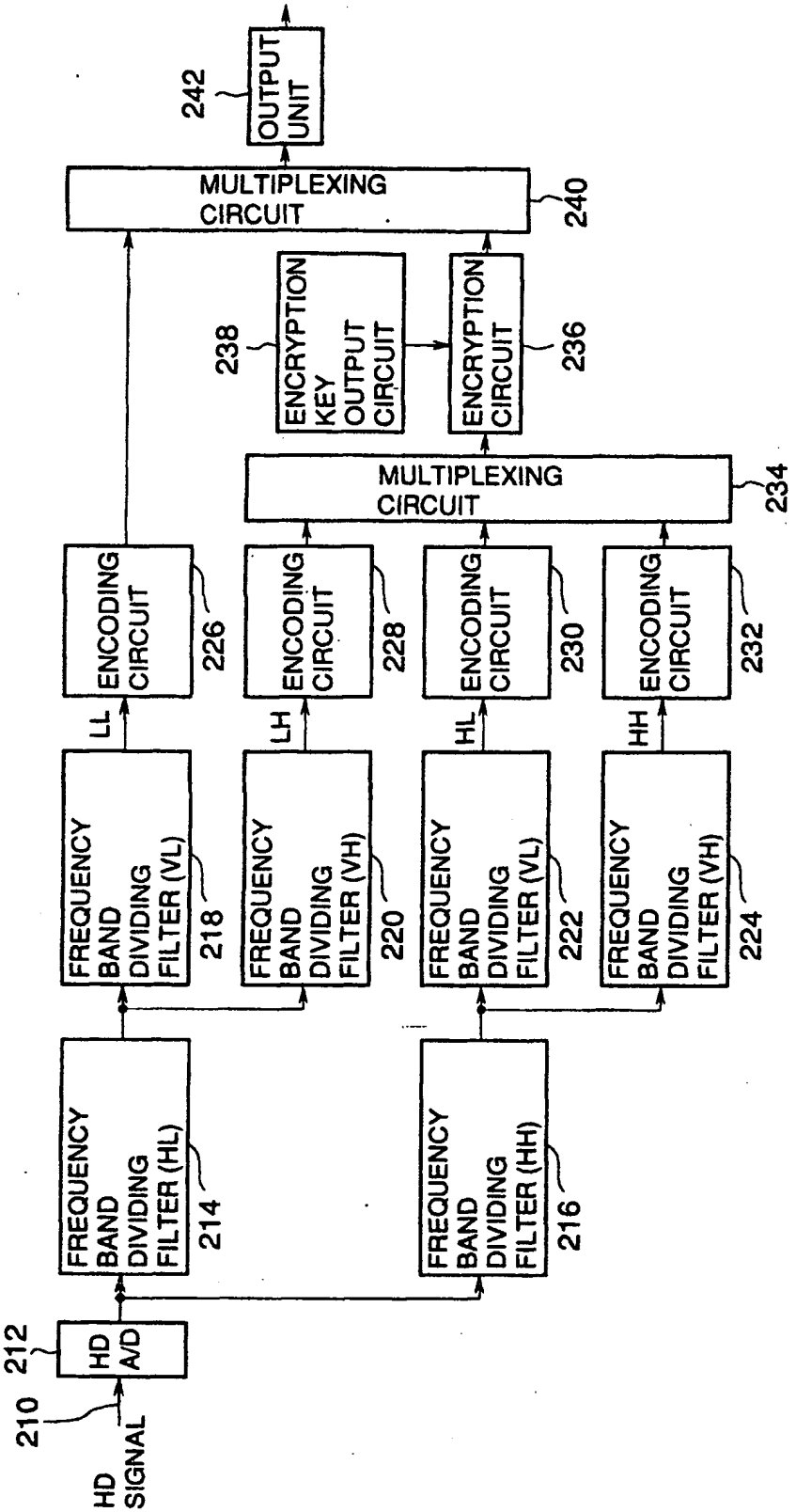

HD SIGNAL
210
HD A/D
212
FREQUENCY BAND DIVIDING FILTER (HL)
214
FREQUENCY BAND DIVIDING FILTER (HH)
216
FREQUENCY BAND DIVIDING FILTER (VL)
218
FREQUENCY BAND DIVIDING FILTER (VH)
220
FREQUENCY BAND DIVIDING FILTER (VL)
222
FREQUENCY BAND DIVIDING FILTER (VH)
224
LL
LH
HL
HH
ENCODING CIRCUIT
226
ENCODING CIRCUIT
228
ENCODING CIRCUIT
230
ENCODING CIRCUIT
232
MULTIPLEXING CIRCUIT
234
ENCRYPTION KEY OUTPUT CIRCUIT
238
ENCRYPTION CIRCUIT
236
MULTIPLEXING CIRCUIT
240
OUTPUT UNIT
242

FIG. 10

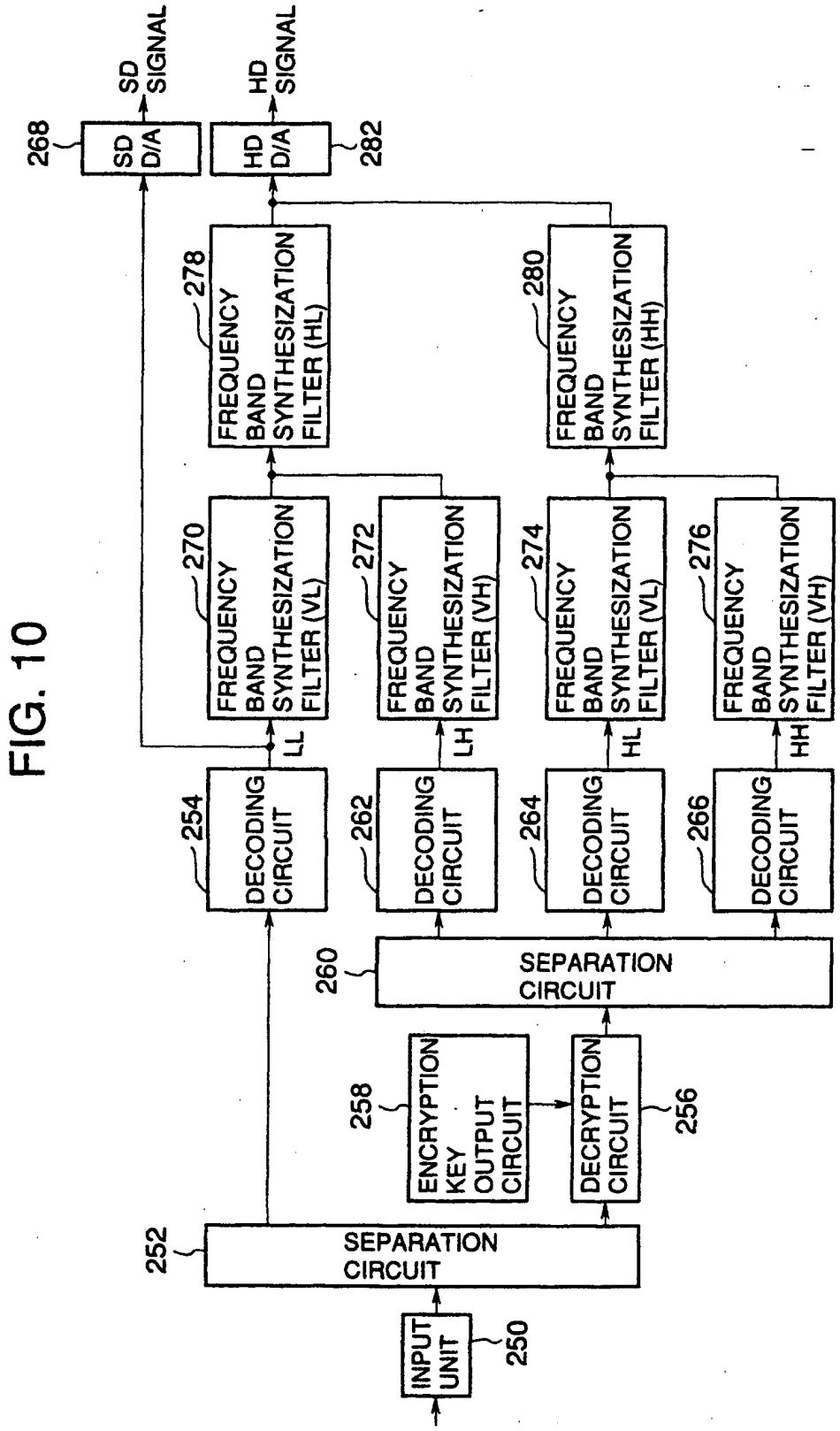

INPUT UNIT
250
SEPARATION CIRCUIT
252
SEPARATION CIRCUIT
260
ENCRYPTION KEY OUTPUT CIRCUIT
258
DECRYPTION CIRCUIT
256
DECODING CIRCUIT
254
DECODING CIRCUIT
262
DECODING CIRCUIT
264
DECODING CIRCUIT
266
LL
LH
HL
HH
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
270
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
272
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
274
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
276
FREQUENCY BAND SYNTHESIZATION FILTER (HL)
278
FREQUENCY BAND SYNTHESIZATION FILTER (HH)
280
SD D/A
268
HD D/A
282
SD SIGNAL
HD SIGNAL

FIG. 11

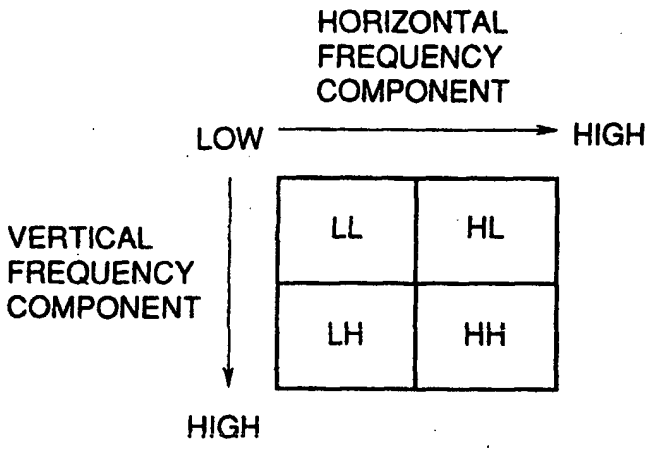

HORIZONTAL
FREQUENCY
COMPONENT
LOW
HIGH
VERTICAL
FREQUENCY
COMPONENT
LL
HL
LH
HH
HIGH

FIG. 12

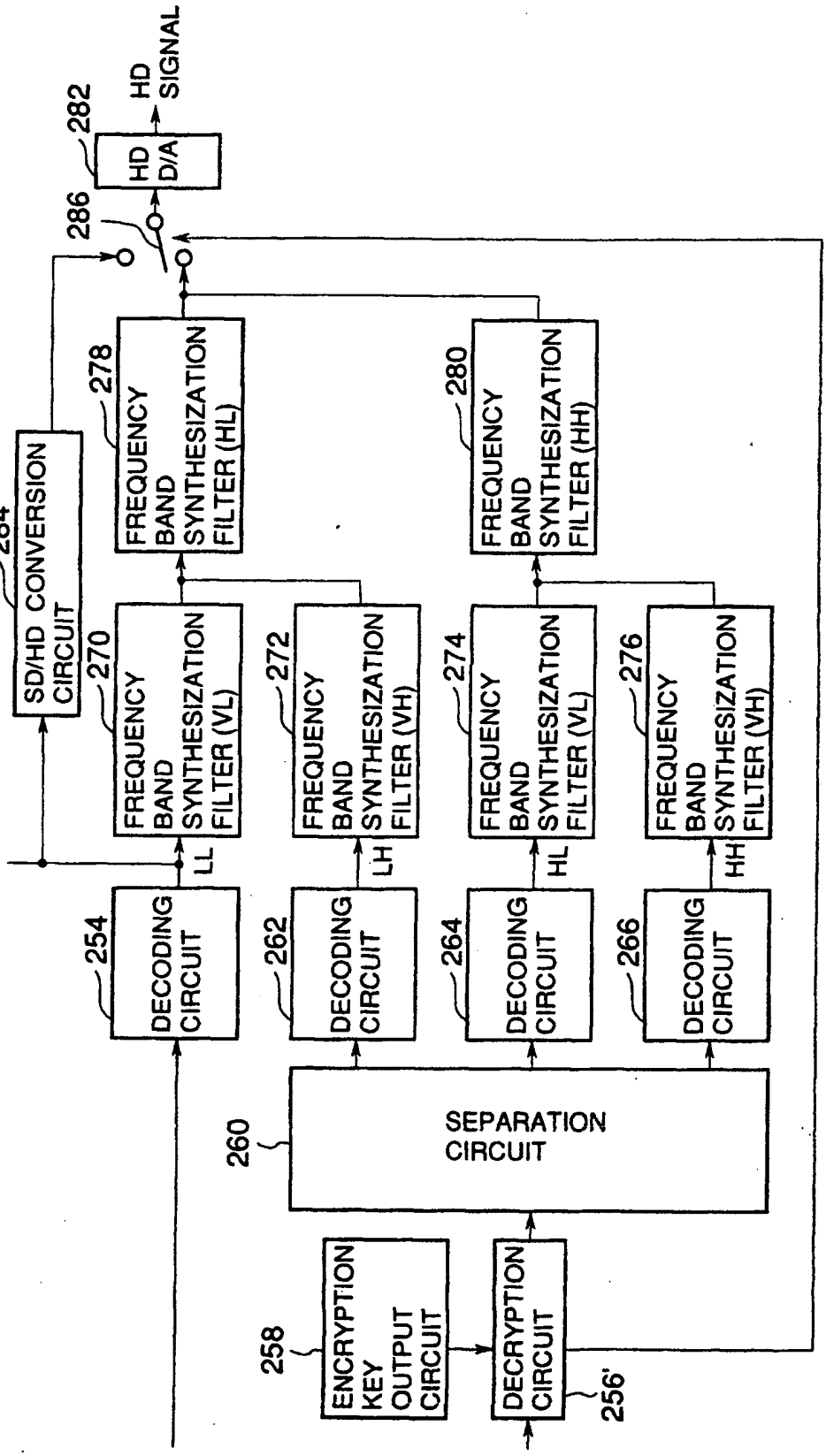

HD SIGNAL
282
HD D/A
286
284
SD/HD CONVERSION CIRCUIT
278
FREQUENCY BAND SYNTHESIZATION FILTER (HL)
280
FREQUENCY BAND SYNTHESIZATION FILTER (HH)
270
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
272
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
274
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
276
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
LL
LH
HL
HH
254
DECODING CIRCUIT
262
DECODING CIRCUIT
264
DECODING CIRCUIT
266
DECODING CIRCUIT
260
SEPARATION CIRCUIT
258
ENCRYPTION KEY OUTPUT CIRCUIT
DECRYPTION CIRCUIT
256'

FIG. 13

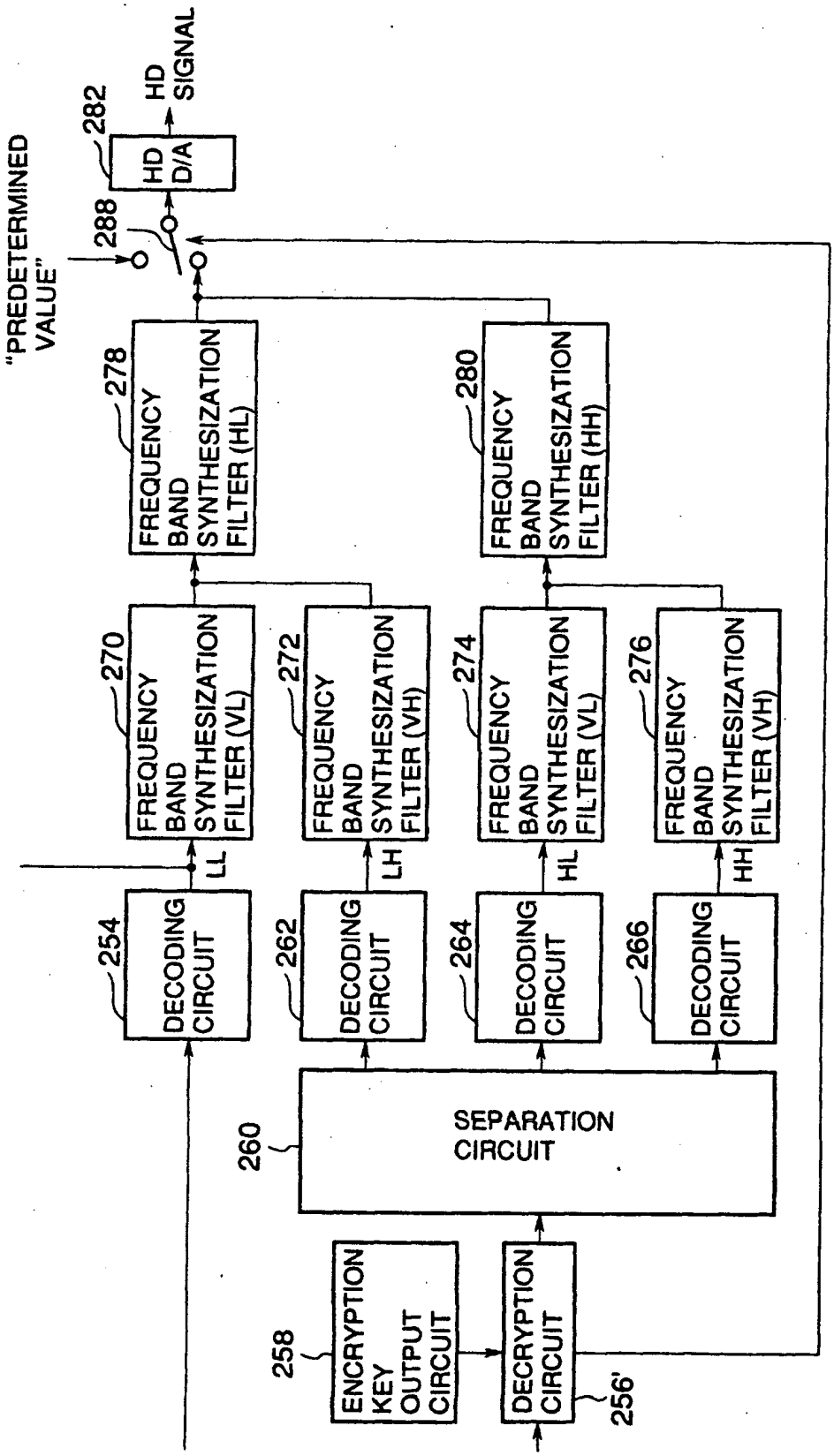

"PREDETERMINED VALUE"
288
282
HD D/A
HD SIGNAL
278
FREQUENCY BAND SYNTHESIZATION FILTER (HL)
280
FREQUENCY BAND SYNTHESIZATION FILTER (HH)
270
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
272
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
274
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
276
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
LL
LH
HL
HH
254
DECODING CIRCUIT
262
DECODING CIRCUIT
264
DECODING CIRCUIT
266
DECODING CIRCUIT
260
SEPARATION CIRCUIT
258
ENCRYPTION KEY OUTPUT CIRCUIT
DECRYPTION CIRCUIT
256'

FIG. 14

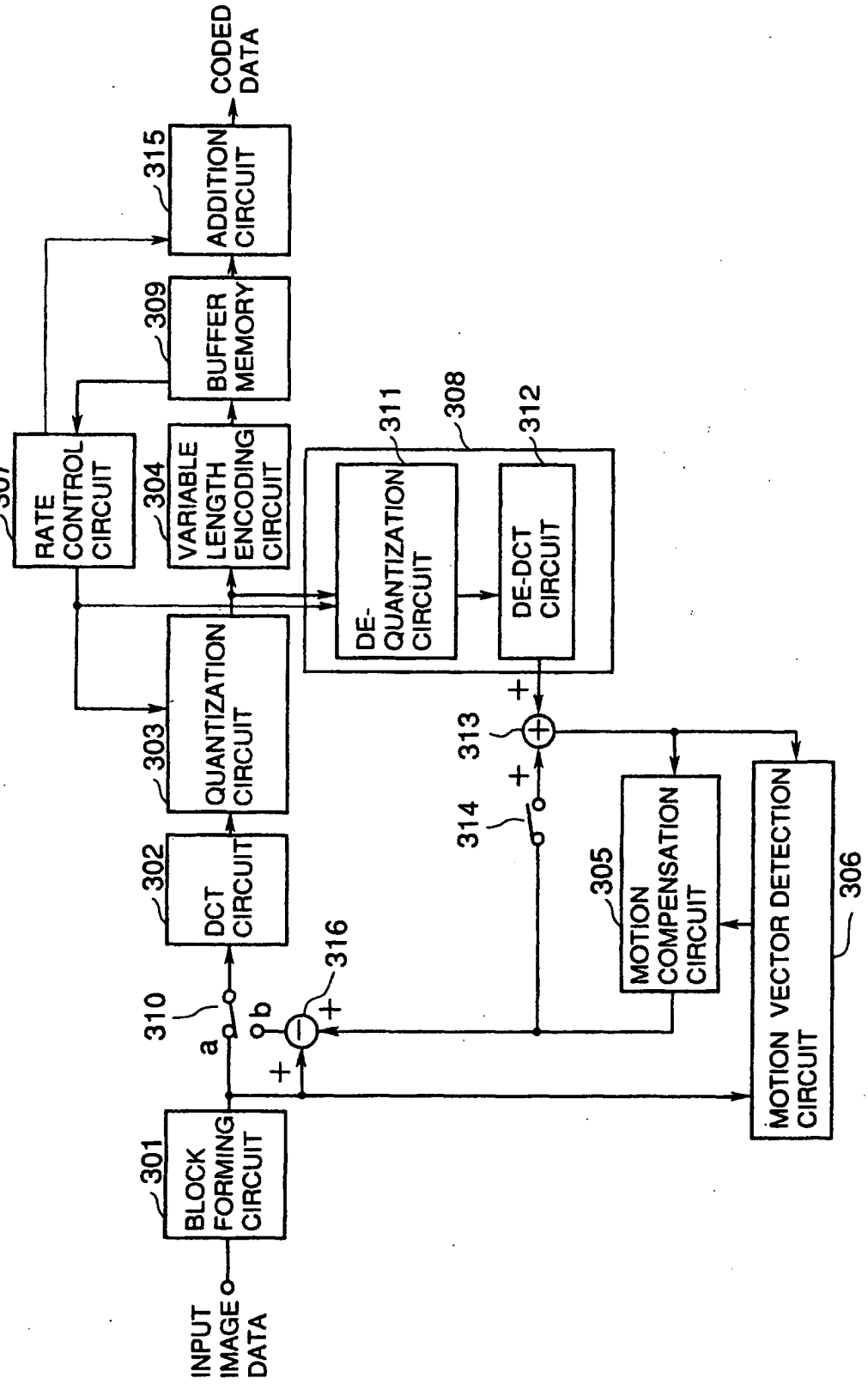
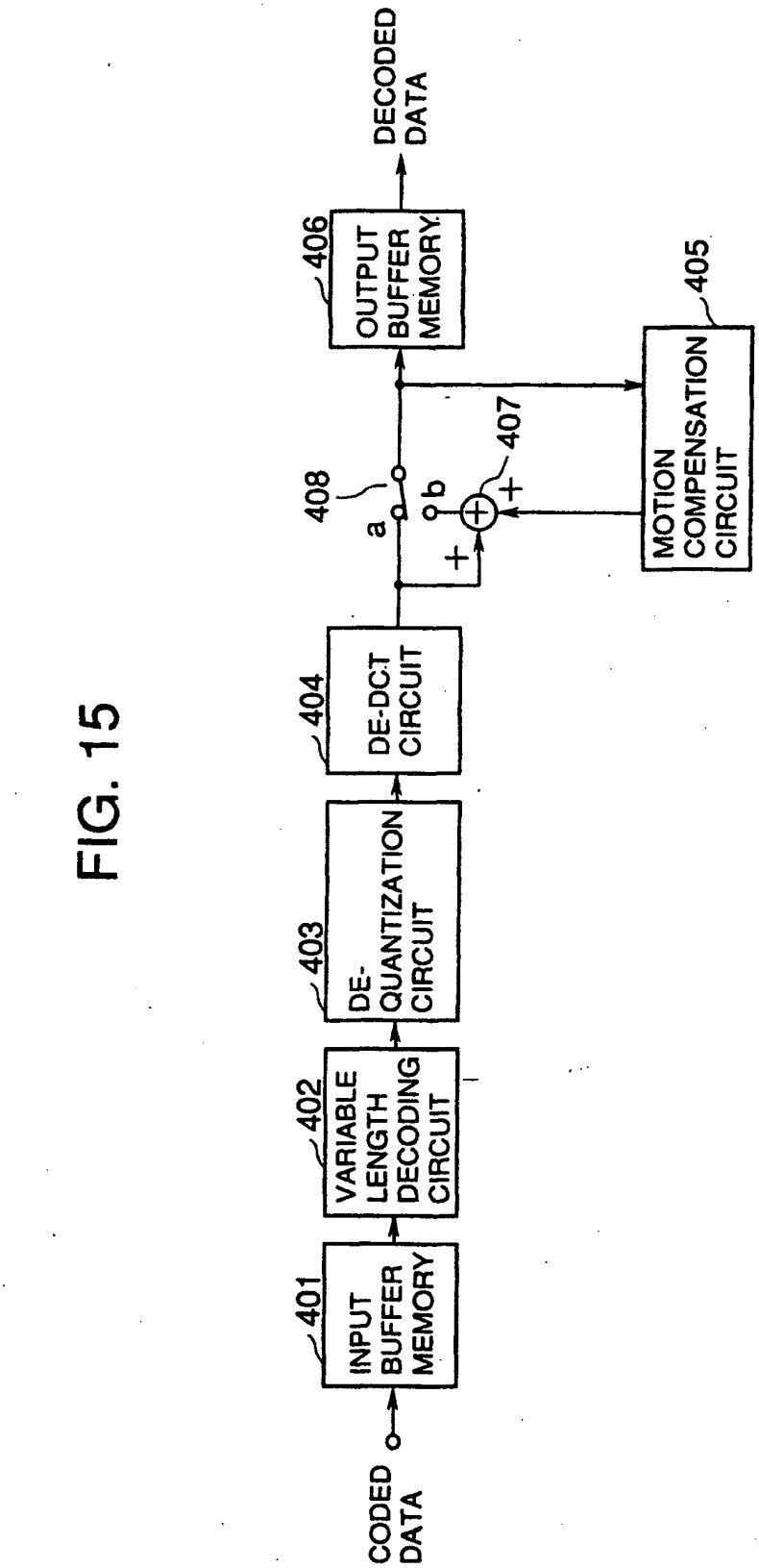

INPUT IMAGE DATA
BLOCK FORMING CIRCUIT
301
DCT CIRCUIT
302
QUANTIZATION CIRCUIT
303
VARIABLE LENGTH ENCODING CIRCUIT
304
MOTION COMPENSATION CIRCUIT
305
MOTION VECTOR DETECTION CIRCUIT
306
RATE CONTROL CIRCUIT
307
DE-QUANTIZATION CIRCUIT
311
DE-DCT CIRCUIT
312
BUFFER MEMORY
309
ADDITION CIRCUIT
315
CODED DATA
310
a
b
314
313
316

FIG. 15


CODED DATA
401
INPUT BUFFER MEMORY
402
VARIABLE LENGTH DECODING CIRCUIT
403
DE-QUANTIZATION CIRCUIT
404
DE-DCT CIRCUIT
408
a
b
+
+
407
406
OUTPUT BUFFER MEMORY
DECODED DATA
405
MOTION COMPENSATION CIRCUIT